Universidade Federal de Santa Maria
Centro de Ciências Naturais e Exatas
Departamento de Matemática

S-Anéis, Anel Centralizador e Grupos com Loops Transversais

Saradia Della Flora †
Mestrado em Matemática - Santa Maria - RS

Orientadora: Prof. Dr. Maria de Lourdes Merlini Giuliani

†Este trabalho teve apoio financeiro da CAPES.

S-Anéis, Anel Centralizador e Grupos com Loops Transversais

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por **Saradia Della Flora** e aprovada pela comissão julgadora.

Santa Maria, 20 de janeiro de 2009.

_____

Prof. Dr. **Maria de Lourdes Merlini Giuliani**.
Orientadora

Banca examinadora:

_____

Prof. Dr. Maria de Lourdes Merlini Giuliani (Orientadora, CCNE - UFSM)

_____

Prof. Dr. Alegria Gladys Chalom (IME - USP)

_____

Prof. Dr. Wagner de Oliveira Cortes (IM - UFRGS)

_____

Prof. Dr. Dirceu Bagio (CCNE - UFSM)

Dissertação apresentada ao Programa de Pós-Graduação em Matemática, UFSM, como requisito parcial para obtenção do título de **Mestre em Matemática**.

Aos meus pais

Agradecimentos

Agradeço primeiramente a Deus, a quem devo tudo. À minha família pelo carinho e incentivo nestes anos de ausência do meu lar. Ao meu noivo Cicero pela força em todos os momentos. Aos meus colegas de Pós-Graduação, em especial à Daiana pela amizade e apoio. Sou grata a minha amiga Vivian pelo companherismo e excelente convívio. Ao curso de Pós-Graduação em Matemática da UFSM pela acolhida e aos professores que contribuiram na minha formação acadêmica. Meu profundo agradecimento a minha orientadora Maria de Lourdes Giuliani pela sugestão do tema e dedicação durante o desenvolvimento desta dissertação. À CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior) pelo auxílio financeiro.

Resumo

Neste trabalho apresentamos os conceitos de loop transversal, anel centralizador e S-anel de um grupo de permutação. As conexões entre esses três tópicos foram obtidos por Kenneth W. Johnson em [6, 7], onde ele adaptou os resultados de Schur e Wielandt de "S-anéis sobre grupos"para "S-anéis sobre loops".

Abstract

In this work, we present the concepts of loop transversal, centralizer ring and S-ring over a permutation group. The connection between these three subjects was obtained by Kenneth W. Johnson, where he translated the results of Schur and Wielandt on "S-rings over groups"to results on "S-rings over loops".

Sumário

Introdução

O conceito de loop transversal é devido à Baer, que em [1] mostrou como loops surgem da generalização de grupos quocientes quando flexibilizamos a exigência da normalidade do subgrupo, ou seja, se um grupo G com um subgrupo H tem uma decomposição em classes laterais à direita de H, $G = He \cup Hx_1 \cup Hx_2 \cup ...$ onde e é o elemento identidade, então é sempre possível definir uma relação binária sobre o transversal $T = \{e, x_1, x_2, ...\}$. Em certos casos essa operação binária torna T um loop, e chamaremos T de *loop transversal*. A questão da existência ou não de tais loops transversais está intimamente ligada às propriedades dos grupos envolvidos. Além disso, podemos considerar a questão inversa: todo loop pode ser considerado como um loop transversal de algum grupo G por um subgrupo H?

O anel centralizador de um grupo de permutação aparece em muitos contextos, como por exemplo na teoria de representação de grupos clássicos sobre corpos finitos ou infinitos onde eles são chamados anéis de Hecke. A estrutura do anel centralizador de um grupo de permutação transitiva finito está estreitamente relacionada com a estrutura algébrica do transversal do estabilizador de um ponto. Em [10, 11], Schur considerou a situação onde um grupo de permutação agindo sobre um conjunto finito Ω tem um subgrupo regular H. Neste caso Ω pode determinar a estrutura do subgrupo H e o anel centralizador de H é isomorfo ao subanel do anel de grupo $\mathbb{Z}H$ que é chamado de S-anel sobre H. Schur usou isto em sua investigação sobre os B-grupos, isto é, os *grupos de Burnside*. Existe uma crescente conexão com anéis centralizadores de grupos de permutação com combinatória e teoria de códigos. O leitor interessado pode consultar [2, 5].

O estudo a respeito dos S-anéis surgiu com Schur [10, 11] e Wielandt [15, 16], e mais tarde foi continuado por Tamaschke e Scott, veja por exemplo [13, 14]. Em [12], Scott formalizou os trabalhos de Schur. Nesta dissertação os resultados de Schur e Wielandt à cerca de "S-anéis sobre grupos"são adaptados para "S-anéis sobre loops".

Capítulo 1

Pré - Requisitos

Neste capítulo relembramos alguns resultados e conceitos clássicos da teoria de grupos e de loops que serão necessários no decorrer deste trabalho. Para maiores detalhes o leitor interessado pode consultar [3, 4, 9].

1.1 Quasigrupos e Loops

Quasigrupos podem ser definidos combinatorialmente ou equacionalmente. Combinatorialmente temos a seguinte definição.

Definição 1.1.1. *Um quasigrupo à direita (à esquerda) é um conjunto Q com uma operação binária $(\cdot)$ tal que para todo $x, y \in Q$ a equação $a \cdot x = y$ $(x \cdot a = y)$ tem uma única solução $a \in Q$. Um quasigrupo à direita e à esquerda é chamado um quasigrupo.*

A definição equacional de quasigrupo descreve-o como álgebra universal com operações de multiplicação $(\cdot)$, left-division $(\backslash)$ e right-division $(/)$.

Definição 1.1.2. *Um quasigrupo $(Q, \cdot, \backslash, /)$ é um conjunto Q com três operações binárias $(\cdot)$, $(\backslash)$, $(/)$ que satisfazem as seguintes identidades:*
(1) $y \setminus (y \cdot x) = x$;
(2) $(x \cdot y)/y = x$;
(3) $y \cdot (y \setminus x) = x$;
(4) $(x/y) \cdot y = x$.

A proposição seguinte mostra a equivalência dessas definições:

Proposição 1.1.3. *O quasigrupo $(Q, \cdot, \backslash, /)$ é um quasigrupo equacional se, e somente se, $(Q, \cdot)$ é um quasigrupo combinatorial.*

Prova: Sejam x,$z \in Q$ e considere a equação:

$$x \cdot y = z. \tag{1.1.1}$$

Tomando $y = x \backslash z$ e usando a equação (3) temos: $x \cdot (x \backslash z) = z$. Assim, a equação 1.1.1 tem solução para $y = x \backslash z$. Seja y' outra solução de 1.1.1. Então

$$y = x \backslash z = x \backslash (x \cdot y') = y'.$$

Logo, a solução $x \backslash z$ é única.
Reciprocamente, suponhamos que $(Q, \cdot)$ é um quasigrupo combinatorial. Para cada $x, y \in Q$, defimos x/y como sendo o único elemento de Q que satisfaz a equação (4):

$$(x/y) \cdot y = x,$$

e defina $y \backslash x$ como sendo a única solução de (3):

$$y \cdot (y \backslash x) = x.$$

Isto define $(/)$ e $(\backslash)$ como operações binárias em Q. Portanto, $(Q, \cdot, /, \backslash)$ é um quasigrupo equacional. □

A tábua abaixo é de um dos menores quasigrupos, cuja ordem é 3:

$\cdot$	1	2	3
1	1	2	3
2	3	1	2
3	2	3	1

Definição 1.1.4. *Um loop é um quasigrupo Q com um elemento identidade e tal que $e \cdot x = x = x \cdot e$, para todo $x \in Q$.*

Usaremos a justaposição ao invés de $(\cdot)$.

Segue direto da definição que num loop Q todo elemento é invertível. Para $x \in Q$, o inverso à esquerda x^λ de x é o único elemento de Q satisfazendo $x^\lambda x = e$. Analogamente, o inverso à direita x^ρ de x é o único elemento de Q satisfazendo $xx^\rho = e$. Se $x^\lambda = x^\rho$ então $x^{-1} = x^\lambda = x^\rho$ é chamado inverso de x. Por exemplo, grupos são exatamente loops associativos.

Considere $(Q, \cdot)$ um loop qualquer, então os cancelamentos à direita e à esquerda são válidos em Q. De fato, sejam $x, y, z \in Q$ tais que $xy = yz$. Como Q é um loop, existe um único $w \in Q$ tal que $yw = e$. Logo, de $xy = zy$ temos $xyw = zyw$, ou seja, $x = z$. Analogamente mostra-se que $xy = xz$ implica que $y = z$.

Um quadrado latino de ordem n é um quadrado $n \times n$ preenchido com n diferentes símbolos de tal maneira que esses ocorrem no máximo uma vez em cada linha ou coluna. A *tábua de Cayley ou tábua de multiplicação* de um loop (ou quasigrupo) finito é um quadrado latino.

Em um loop qualquer $(Q, \cdot)$, definimos as translações à direita $R(x)$ e à esquerda $L(x)$ por:

$$R(x) : y \mapsto yx \qquad L(x) : y \mapsto xy$$

para todo $y \in Q$. Na teoria de loops, é comum escrever a função à direita de seus argumentos.

A definição de loop finito é equivalente a afirmação de que $R(x)$ e $L(x)$ são bijeções de Q, para todo $x \in Q$. As translações à direita, por exemplo, são injetoras já que vale o cancelamento em Q, e também sobrejetoras, pois se $y \in Q$ a definição de quasigrupo assegura a existência de $z \in Q$ tal que $zx = y$. Portanto, o conjunto das translações à direita e à esquerda gera um grupo $M(Q)$ chamado *grupo multiplicativo de* Q, que é um subgrupo do grupo simétrico no conjunto Q. Assim:

$$M(Q) =< R(x), L(x); x \in Q >.$$

Definição 1.1.5. *Um subloop P de um loop $(Q, .)$ é um subconjunto de Q que, sob a operação binária herdada é também um loop.*

Desde que, para cada $p \in P$ a equação $px = p$ tem solução única em Q, segue que o elemento identidade de P e de Q são os mesmos.

Definição 1.1.6. *Sejam Q_1 e Q_2 loops. A função $f : Q_1 \to Q_2$ é um homomorfismo de loops se satisfaz $f(xy) = f(x)f(y)$, para todo $x, y \in Q_1$. Além disso, quando o homomorfismo f é bijetora dizemos que f é um isomorfismo.*

1.2 Ação de Grupo em um Conjunto

Nesta seção apresentamos o conceito de ação de grupo com alguns resultados e definições que decorrem deste. Apesar de clássica, a ação de grupo sobre um conjunto

será uma ferramenta fundamental neste trabalho.

Definição 1.2.1. *Sejam G um grupo e X um conjunto. Uma ação de G em X é uma função:*

$$\begin{array}{rccc} \varphi & : & G \times X & \longrightarrow & X \\ & & (g, x) & \longmapsto & gx \end{array}$$

tal que para todo $x \in X$ e para todo $g, h \in G$:
(1) $ex = x$
(2) $(gh)x = g(hx)$
onde e é o elemento neutro de G.

Exemplos: (1) O grupo simétrico S_n age no conjunto $\{1, 2, \ldots, n\}$.
(2) Seja G um grupo e $X = G$. A função:

$$\begin{array}{rccc} \varphi & : & G \times X & \longrightarrow & X \\ & & (g, x) & \longmapsto & gxg^{-1} \end{array}$$

é uma ação de G em G chamada ação por conjugação.

Considere o grupo G agindo num conjunto X e $x \in X$. Para cada $x \in X$, podemos definir dois importantes subconjuntos: a *órbita* e o *estabilizador* de x.
A *órbita* de x, denotada por $\mathcal{O}(x)$, é o conjunto:

$$\mathcal{O}(x) = \{gx; g \in G\} \subset X.$$

Nessas mesmas condições, o *estabilizador* de x, denotado por G_x, é o subgrupo de G:

$$G_x = \{g \in G; gx = x\}.$$

Se para algum $x_0 \in X$ tivermos $G_{x_0} = G$, dizemos que x_0 é um ponto fixo pela ação de G.

Se H é um subgrupo do grupo G então denotaremos por $[G : H]$ o *índice* de H em G, isto é, o número de classes laterais de H em G. O resultado seguinte é bastante conhecido na teoria de grupos sobre conjuntos. Uma demostração pode ser vista em [9, Teorema 3.19].

Teorema 1.2.2. *Se o grupo G age sobre um conjunto X e $x \in X$ então $|\mathcal{O}(x)| = [G : G_x]$.*

Definição 1.2.3. *Uma ação de um grupo G num conjunto X é dita transitiva se ocorre uma (e portanto todas) das três condições equivalentes:*
(1) *Existe $x \in X$ tal que $\mathcal{O}(x) = X$.*
(2) *Para todo $x, y \in X$ existe $g \in G$ tal que $x = gy$.*
(3) *Para todo $x \in X$, $\mathcal{O}(x) = X$.*

Vejamos um exemplo interessante de ação transitiva: seja H um subgrupo de um grupo G e X o conjunto das classes laterais (à direita) de H em G. Então:

$$\begin{array}{rccc} \varphi & : & G \times X & \longrightarrow & X \\ & & (g, Hx) & \longmapsto & Hxg^{-1} \end{array}$$

define uma ação de G em X que é chamada de ação por translação nas classes laterais.

Se G age nos conjuntos X e Y, então podemos considerar a ação de G no produto cartesiano $X \times Y$ com a chamada *ação diagonal*: $g(x, y) = (gx, gy)$.

Proposição 1.2.4. *Se um grupo G age transitivamente em um conjunto X então todos os estabilizadores de pontos de X são conjugados entre si.*

Prova: Sejam $x, y \in X$ e $g \in G_y$. Como a ação de G em X é transitiva então existe $a \in G$ tal que $y = ax$. Daí, $gy = gax = ax$, isto é, $(a^{-1}ga)x = x$. Assim, $a^{-1}G_y a \subseteq G_x$ e de maneira análoga, temos que $G_x \subseteq a^{-1}G_y a$. Logo, $a^{-1}G_y a = G_x$ como queríamos. □

Teorema 1.2.5. *(Lema de Burnside) Se G um grupo finito agindo num conjunto finito X e N o número de órbitas de X. Então:*

$$N = \left(\frac{1}{|G|}\right) \sum_{g \in G} F(g)$$

onde, para $g \in G$, $F(g)$ é o número de elementos de X que são fixados por g.

Prova: Na soma $\sum_{g \in G} F(g)$, cada elemento $x \in X$ é contado $|G_x|$ vezes.
Se x e y estão numa mesma órbita então $|G_x| = |G_y|$, e assim os $[G : G_x]$ elementos constituindo a órbita de x são contados coletivamente $[G : G_x]|G_x| = |G|$ vezes. Como cada órbita contribui com $|G|$ na soma, então $\sum_{g \in G} F(g) = N|G|$. Portanto, $N = 1/|G| \sum_{g \in G} F(g)$ □

Corolário 1.2.6. *Se G é um grupo agindo transitivamente em um conjunto finito X, com $|X| > 1$ então existe $g \in G$ que não fixa nenhum elemento de X.*

Prova: Temos que o número de órbitas N de X é igual a 1, uma vez que a ação é transitiva. Pelo teorema acima,

$$1 = \left(\frac{1}{|G|}\right) \sum_{g \in G} F(g).$$

Seja $|G| = k$. Como $F(e) = |X| > 1$ então suponhamos que $F(g) \geq 1$, para todo $g \in G$. Logo, $\sum_{g \in G} F(g) = F(e) + F(g_2) + \cdots + F(g_k) > k = |X|$.
Portanto, $(\sum_{g \in G} F(g))/|G| > 1$, o que é um absurdo, e portanto, existe $g \in G$ tal que $F(g) = 0$. □

Suponhamos que G age em um conjunto finito X, onde $|X| \geq 2$. A ação é dita *2-transitiva* (ou duplamente transitiva), se quando (x_1, x_2) e (y_1, y_2) são pares de elementos distintos de X, existe $g \in G$ tal que $gx_1 = y_1$ e $gx_2 = y_2$. A ação é dita *k-transitiva* (ou multiplamente transitiva), se para todo par de k-uplas com entradas distintas, digamos $(x_1, x_2, \ldots, x_k)$ e $(y_1, y_2, \ldots, y_k)$, existe $g \in G$ tal que $gx_i = y_i$, para todo $i = 1, 2, \ldots, k$.

Suponhamos que G age em um conjunto finito X. Um subconjunto B de X é dito um *bloco* (ou conjunto de imprimitividade) para a ação se, para cada $g \in G$, ou $gB = B$ ou $gB \cap B = \emptyset$ ($gB = \{gx; x \in B\}$). Em particular, $\emptyset$, X e subconjuntos de X formados por um único ponto são obviamente blocos e são chamados *blocos triviais*. No caso particular em que G age transitivamente em um conjunto X, dizemos que a ação é *primitiva* se os únicos blocos são os blocos triviais. Caso contrário a ação é *imprimitiva*. O grupo G é um *grupo primitivo* se G age primitivamente em X, isto é, para todo $B \subset X$, não trivial, existe $g \in G$ tal que $gB \cap B \neq \emptyset$ e $gB \neq B$. O grupo G é dito *imprimitivo* se existe $B \subseteq X$ tal que, para todo $g \in G$, $gB = B$ ou $gB \cap B = \emptyset$.

Toda partição $\{B_1, \ldots, B_m\}$ de um conjunto X define uma relação de equivalência $\equiv$ em X onde as classes de equivalência são exatamente os B_i. Em particular, se G age em um conjunto finito X e B é um bloco então existe uma relação de equivalência em X dada por:

$x \equiv y$ se existem $g \in G$ e B um bloco de X tal que gB contém x e y.

Esta relação é G-invariante, isto é, se $x \equiv y$ então $gx \equiv gy$, para todo $g \in G$. Por outro lado, se $\equiv$ é uma relação de equivalência G-invariante em X então qualquer classe de equivalência é um bloco. Assim, G é primitivo se, e somente se, ele admite uma relação de equivalência G-invariante trivial.

Teorema 1.2.7. *Seja G grupo agindo sobre um conjunto X. Se G é duplamente transitivo então G é primitivo.*

Prova: Se X tem um bloco não trivial B, então existem elementos $x, y, z \in X$ com $x, y \in B$ e $z \notin B$. Como G é duplamente transitivo, existe $g \in G$ tal que $gx = x$ e $gy = z$. Assim, $x \in B \cap gB$ e $B \neq gB$, o que é um absurdo. Logo, X possui somente blocos triviais, e portanto, G é primitivo. □

Teorema 1.2.8. *Sejam G um grupo agindo transitivamente em conjunto finito X de ordem n e B um bloco não trivial de X. São válidos:*
(i) Se $g \in G$ então gB é um bloco.
(ii) Existem elementos $g_1, \ldots, g_m$ de G tais que $Y = \{g_1B, \ldots, g_mB\}$ é uma partição de X.
(iii) $|B|$ divide n, e G age transitivamente em Y onde a ordem de Y é $m = \dfrac{n}{|B|}$.

Prova:
(i) Se $gB \cap hgB \neq \emptyset$, para algum $h \in G$, então $B \cap g^{-1}hgB \neq \emptyset$. Como B é um bloco, $g^{-1}hgB = B$, e daí, $gB = hgB$. Portanto, gB é um bloco de X.

(ii) Se X tem ordem 1 então $gX = X$ é um bloco trivial. Podemos assumir que a ordem de X é maior ou igual a 2. Tome $b \in B$ e $x_1 \notin B$. Por hipótese, G age transitivamente em X. Assim, existe $g_1 \in G$ com $g_1b = x_1$. Se $g_1B = B$ então $g_1b \in B$. Dessa forma, $x_1 \in B$ o que é um absurdo. Logo, como B é um bloco, temos que $g_1B \cup B = \emptyset$. Se $X = B \cup g_1B$ então o resultado se verifica. Caso contrário, tome $x_2 \notin B \cup g_1B$ e $g_2 \in G$ tal que $g_2b = x_2$. É fácil ver que $x_2 \in g_2B$, $x_2 \notin B$ e $x_2 \notin g_1B$. Portanto, $g_2B \neq B$ e $g_2B \neq g_1B$. Assim, $g_2B \cap (B \cup g_1B) = \emptyset$, já que B e g_1B são blocos. Continuando esse processo obtemos o resultado.

(iii) Note que $|B| = |g_iB|$, para todo $i = 1, 2, \ldots, m$, e que $n = |X| = m|B|$. Consequentemente, $|B|$ divide n e $|Y| = m = \dfrac{n}{|B|}$.
Para verificar que G age transitivamente em Y, considere g_iB e $g_jB \in Y$, $x \in B$.

Pela transitividade da ação de G em X, existe $g \in G$ tal que $gg_ix = g_jx$, ou seja, $\emptyset \neq gg_iB \cap g_jB = (gg_ig_j^{-1})g_jB \cap g_jB$. Como g_jB é um bloco então $gg_iB = g_jB$. □

Corolário 1.2.9. *Se G age transitivamente em um conjunto X tal que $|X|$ é um número primo então G é primitivo.*

Prova: Segue diretamente do item (iii) do teorema acima. □

Existe uma caracterização para os grupos primitivos dada através do seguinte teorema:

Teorema 1.2.10. *Suponha que G age transitivamente em um conjunto X. Então G é primitivo se, e somente se, para cada $x \in X$, G_x é um subgrupo maximal de G.*

Prova: ($\Rightarrow$) Suponhamos que G_x não é maximal, isto é, existe um subgrupo H tal que $G_x < H < G$. Iremos mostrar que $Hx = \{gx; g \in H\}$ é um bloco não trivial.
De fato, se $g \in G$ e $Hx \cap gHx \neq \emptyset$ então $hx = gh'x$, com $h, h' \in H$. Como $h^{-1}gh'$ fixa x então $h^{-1}gh' \in G_x < H$, e com isto, $g \in H$. Assim, $gHx = Hx$ e Hx é um bloco. Resta mostrar que Hx é não trivial. Claramente Hx é não vazio. Seja $g \in G$, com $g \notin H$. Se $Hx = X$ então, para todo $y \in X$, existe $h \in H$ tal que $y = hx$. Em particular, $gx = hx$ para algum $h \in H$. Logo, $g^{-1}h \in G_x < H$, e assim $g \in H$, o que é um absurdo.
Finalmente, se Hx é um conjunto unitário então $H \leq G_x$ contradizendo o fato de que $G_x < H$. Portanto, G é imprimitivo.
($\Leftarrow$) Suponhamos que todo subgrupo G_x é maximal em G e que existe um bloco não trivial B em X. Defimos o subgrupo H de G por: $H = \{g \in G; gB = B\}$. Tome $x \in B$.
Se $gx = x$ então $x \in B \cap gB$, e portanto, $gB = B$. Logo, $G_x \leq H$. Como B é não trivial, existe $y \in B$, $y \neq x$. Pela transitividade da ação, existe $g \in G$ tal que $gx = y$. Assim, $y \in B \cap gB$, e consequentemente, $gB = B$. Logo, $g \in H$ e $g \notin G_x$, isto é, $G_x < H$.
Se $H = G$ então $gB = B$, para todo $g \in G$, e isto contradiz o fato de que $X \neq B$. Portanto, $G_x < H < G$ contradizendo a maximalidade de G_x. Logo, B é um bloco trivial e G é um grupo primitivo. □

Definição 1.2.11. *Um subgrupo H de um grupo G é dito regular se H é livre de ponto fixo, isto é, $G_h = \{e\}$, para todo $h \in H$.*

Definição 1.2.12. *Seja G um grupo de permutação transitiva sobre X e que possui um subgrupo regular H. O subgrupo H é dito um grupo de Burnside ou B-grupo se G é imprimitivo ou duplamente transitivo.*

Wielandt provou que o grupo diedral D_n é um grupo de Burnside. Na prova desse resultado utilizou o teorema de Dirichlet para primos em progressão aritmética.

1.3 Representação de Grupos Finitos

Nesta seção G denotará um grupo finito multiplicativo com elemento identidade e, V espaço vetorial de dimensão finita sobre o corpo dos números complexos $\mathbb{C}$. Denotaremos por $GL_n(\mathbb{C})$ o conjunto das matrizes inversíveis de ordem n com entradas complexas e, por $GL(V)$ o conjunto de todas as transformações lineares inversíveis de V em V.

Definição 1.3.1. *Uma representação de G com espaço de representação V é um homomorfismo de grupos:*

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

Duas representações T e T' com espaços de representação V e V' são ditas *equivalentes* se existe um isomorfismo S entre os espaços vetorias V e V' tal que:

$$T'(g)S = ST(g), \text{ para todo } g \in G.$$

A dimensão de V sobre $\mathbb{C}$ é chamado *grau* de T.

Analogamente, temos o conceito de *representação matricial*:

Definição 1.3.2. *Uma representação matricial de G de grau n é um homomorfismo de grupos:*

$$\begin{array}{rccc} T: & G & \longrightarrow & GL_n(\mathbb{C}) \\ & g & \longmapsto & [T(g)] \end{array}$$

Duas representações matriciais $[T]$ e $[T]'$ são equivalentes se elas possuem mesma ordem, digamos n, e se existe uma matriz fixada $[S] \in GL_n(\mathbb{C})$ tal que

$$[T'(g)] = [S][T(g)[S]^{-1}, \text{ para todo } g \in G.$$

Se T é uma representação de G com espaço V, então das propriedades de homomorfismo decorrem:
(1) $T(e) = 1_V$
(2) $T(g) \circ T(h) = T(gh)$
(3) $T(g)^{-1} = T(g^{-1})$
para todo $g, h \in G$, onde 1_V denota a transformação identidade de V. As correspondentes propriedades valem, obviamente, para as representações matriciais.

O *núcleo* da representação T é o conjunto: $KerT = \{g \in G; T(g) = 1_V\}$. Uma representação é dita *fiel* se $KerT = \{e\}$.

Sejam $T : G \to GL(V)$ uma representação de G e $\{u_1, u_2, \ldots, u_n\}$ uma base de V sobre $\mathbb{C}$. Para cada $g \in G$, a matriz $[T(g)]$ de $T(g)$ com respeito a base $\{u_1, u_2, \ldots, u_n\}$ pertence a $GL_n(\mathbb{C})$, e

$$T : g \to [T(g)]$$

define representação matricial de G chamada de *representação matricial associada à* T. A representação T associa-se a outras representações matriciais mediantes a escolha de outras $\mathbb{C}$-bases de V. Porém, observe que todas essas representações matriciais são equivalentes.

Exemplo (*Representação de Permutação):* Sejam S_n o grupo simétrico com n símbolos e V espaço vetorial sobre $\mathbb{C}$ de dimensão n com base $\{u_1, u_2, \ldots, u_n\}$. Considere a função $P : S_n \longrightarrow GL(V)$ que para cada $\sigma \in S_n$ associa $P(\sigma) : V \longrightarrow V$, dada por $P(\sigma)(u_i) = u_{\sigma(i)}$, para todo $i = 1, 2, \ldots, n$.
Para quaisquer $\sigma, \tau \in S_n$ temos que: $P(\sigma\tau)u_i = u_{\sigma\tau(i)} = u_{\sigma(\tau(i))} = P(\sigma)P(\tau)u_i$, para todo $i = 1, 2, \ldots, n$. Como cada u_i faz parte da base de V, concluimos que $P(\sigma\tau) = P(\sigma)P(\tau)$. Mais ainda, se $P(\sigma) = 1$ então $\sigma = 1$, o que mostra que a função $\sigma \to P(\sigma)$ é um isomorfismo de S_n em $GL_n(\mathbb{C})$.

Seja $[P(\sigma)]$ a matriz de $P(\sigma)$ relativa a base $\{u_1, u_2, \ldots, u_n\}$ de V. Então, $[P(\sigma)]$ é dita *representação matricial de permutação* e é caracterizada pelo fato de que em cada linha e em cada coluna existe uma única entrada diferente de zero, que é igual a 1. A função $\sigma \to [P(\sigma)]$ é um isomorfismo de S_n no subgrupo das matrizes de permutação.

Agora, seja G um grupo de ordem n. Pelo Teorema de Cayley, existe um homomorfismo injetor $\varphi : G \to S_n$. Portanto a função: $R : g \to P(\varphi(g))$ é um isomorfismo de G em $GL(V)$. O isomorfismo R é dito a *representação regular de* G, e é o mais importante exemplo de representação.

Suponhamos que $G = \{g_1, g_2, \ldots, g_n\}$ é um grupo finito de ordem n e $\{u_1, u_2, \ldots, u_n\}$ uma base de V. Para cada i, $1 \leq i \leq n$ e $g \in G$, existe um único $1 \leq j \leq n$ tal que $gg_i = g_j$. Assim, temos $R(g)(u_i) = u_j$. A representação matricial R relativa a base $\{u_1, u_2, \ldots, u_n\}$ é chamada *representação matricial regular* de G.

Evidentemente, para obter uma representação matricial de um grupo arbitrário G, é suficiente encontrar as matrizes que correspondem ao conjunto de geradores de G. Por exemplo, para encontrar a representação matricial regular R do grupo cíclico de ordem n, $C_n =< g; g^n = e >= \{e, g, g^2, \ldots, g^{n-1}\}$, é suficiente encontrar $[R(g)]$, pois g é o gerador de G:

$$R(g) = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}$$

Uma pergunta natural que surge é a seguinte: dada uma representação, será que é possível escrevê-la de forma mais simples?

Definição 1.3.3. *Sejam $T : G \to GL_n(V)$ uma representação de G e W um subespaço de V tal que $T(g)w \in W$, para todo $g \in G$ e para todo $w \in W$. Tal subespaço é chamado subespaço G-invariante.*

Se definirmos

$$T_1(g) = T(g)|W \tag{1.3.2}$$

onde $T(g)|W$ denota a restrição de $T(g)$ em W, então T_1 é uma representação de G com espaço de representação W.

Definição 1.3.4. *Uma representação T de G com espaço de representação V não nulo é irredutível se os únicos subespaços G-invariantes de V são $\{0\}$ (espaço nulo) e V. Caso contrário, T é chamada redutível. A representação T é completamente redutível se para todo subespaço G-invariante W de V, existe um outro subespaço W' tal que $V = W \oplus W'$.*

Sejam $T : G \to GL(V)$ uma representação de G e W um subespaço G-invariante de V tal que $W \neq 0$ e $W \neq V$. Então podemos escolher bases tal que

$$V = \mathbb{C}u_1 \oplus \ldots \oplus \mathbb{C}u_r,\ W = \mathbb{C}u_1 \oplus \ldots \oplus \mathbb{C}u_s, \text{ com } s < r.$$

Com relação a essas bases, V assume a representação matricial $[T]$, digamos, e W a representação matricial $[T_1]$. Temos que para cada $g \in G$,

$$T(g) = \begin{bmatrix} T_1(g) & V(g) \\ 0 & T_2(g) \end{bmatrix} \tag{1.3.3}$$

Observe que existe uma representação $T_2 : G \to GL(V/W)$ definida por:

$$T_2(g)(u + W) = T(g)u + W. \tag{1.3.4}$$

A função $T_2(g)$ está bem definida e é um $\mathbb{C}$-homomorfismo de V/W em si mesmo pois W é um subespaço G-invariante de V. As classes $\{u_{s+1} + W, \ldots, u_r + W\}$ formam uma base para V/W , e claramente T_2 assume a representação matricial $[T_2]$ relativa a essa base.

Se $[T']$ é uma outra representação matricial qualquer de G associada a T, existe uma matriz $[S] \in$ tal que $[S][T'(g)][S]^{-1}$ tem a forma (1.3.3) para todo $g \in G$.

Agora, suponha que V é completamente redutível. Então podemos escrever: $V = W \oplus W'$, $W = \mathbb{C}u_1 \oplus \ldots \oplus \mathbb{C}u_s$, $W' = \mathbb{C}u_1 \oplus \ldots \oplus \mathbb{C}u_r$, e relativo à base $\{u_1, \ldots, u_r\}$, T assume a representação matricial

$$T'(g) = \begin{bmatrix} T_1(g) & 0 \\ 0 & T_2'(g) \end{bmatrix} \tag{1.3.5}$$

É fácil verificar que as representações matriciais $[T_2]$ e $[T_2']$ são equivalentes. Assim, a redutibilidade completa de T implica que cada representação matricial (1.3.3) é equivalente a uma da forma (1.3.5).

Em termos da representação matricial, temos que se encontrarmos uma base em que todas as matrizes da representação podem ser escritas da forma (1.3.3), para todo $g \in G$, então dizemos que a representação T é *redutível*. Se tal redução não existe então $[T]$ é uma representação matricial irredutível. Quando $V(g) = 0$ a representação matricial é dita completamente redutível.

O próximo resultado é clássico da teoria de representações para grupos finitos. Uma demonstração pode ser encontrada em [3].

Teorema 1.3.5. *Toda representação de G é escrita como soma direta de representações irredutíveis de G.*

Capítulo 2

Loop Transversal de um Grupo

Neste capítulo tratamos a respeito da teoria de transversais, loops e grupos de translações. Definimos transversal para grupos e damos condições para que esse possua estrutura de loop. Reciprocamente, mostramos que dado um loop podemos considerá-lo como um loop transversal de algum grupo. Investigamos propriedades dos loops transversais bem como alguns exemplos. Os principais resultados aqui desenvolvidos foram obtidos por Johnson em [6, 7].

2.1 Loop Transversal

Para esta seção, iremos fixar as seguintes notações: G é um grupo multiplicativo com elemento identidade e, H subgrupo qualquer de G. Além disso, usaremos a definição combinatorial de quasigrupo.

Definição 2.1.1. *Um transversal à direita T para H é um sistema completo de representantes das classes laterais à direita de H, tal que $e \in T$.*

Analogamente, definimos um transversal à esquerda para H. Neste capítulo estudaremos sempre transversais à direita, não havendo perigo de confusão usaremos simplesmente a expressão transversal.

Assim, $G = \cup Hx$ onde essa união é disjunta e x percorre todos os elementos de T. Uma operação binária $(\circ)$ pode ser definida em T da seguinte maneira: se $x_i, x_j \in T$ então $x_i x_j = h x_k$, onde $h \in H$ e $x_k \in T$ é único. Assim, definimos

$$x_i \circ x_j = x_k.$$

Observe que em geral, $x_i x_j \neq x_i \circ x_j$.

Proposição 2.1.2. *Seja T um transversal à direita de H em G. O sistema $(T, \circ)$ é um quasigrupo à direita com elemento identidade e.*

Prova:

Sejam $T = \{x_1 = e, x_2, \ldots\}$ um transversal à direita de H em G e $x_i, x_j \in T$. Considere a equação:

$$a \circ x_i = x_j \tag{2.1.1}$$

Como $G = \cup H x_i$, existe $x_k \in T$ tal que $x_j x_i^{-1} = h x_k$, onde $h \in H$. Assim, $x_j = h x_k x_i$, ou seja, $h^{-1} x_j = x_k x_i$. Logo, $x_k \circ x_i = x_j$ e a equação 2.1.1 admite solução. Suponhamos que essa solução não é única, isto é, existe $x_m \in T$ tal que $x_m \circ x_i = x_j$. Então, $x_m x_i = h_1 x_j$, onde $h_1 \in H$. Portanto, $x_m x_i = h_1 h x_k x_i$, ou seja, $x_m = h_2 x_k$ com $h_2 = h_1 h \in H$. Segue que $x_m = x_k$, pois T é um transversal de H em G. Logo, $(T, \circ)$ é um quasigrupo à direita.
Mostremos que e é elemento identidade de $(T, \circ)$. De fato, seja $x_i \in T$ tal que $x_i \circ e = x_j$. Assim, $x_i = h x_j$, ou equivalentemente, $x_j = h^{-1} x_i$. Como T é um transversal, $x_j = x_i$. □

Como vimos, a operação $(\circ)$ define uma estrutura de quasigrupo à direita em T, ou seja, o cancelamento à direita é válido em T. Porém, o cancelamento à esquerda não necessariamente se verifica como podemos ver no seguinte exemplo: considere $G = S_3$, o grupo simétrico com 3 elementos, o subgrupo $H = \{e, (23)\}$ e um transversal $T = \{e, (12), (13)\}$ de H em G. Podemos ver na tábua de multiplicação para $(T, \circ)$, descrita abaixo, que o cancelamento à esquerda não é válido:

$\circ$	e	(12)	(13)
e	e	(12)	(13)
(12)	**(12)**	e	**(12)**
(13)	**(13)**	**(13)**	e

Note que essa tábua não é um quadrado latino.

Dizemos que T é um *loop transversal à direita* se $(T, \circ)$ é um loop, ou seja, $(T, \circ)$ também possui o cancelamento à esquerda. Analogamente, definimos loop transversal à esquerda quando consideramos um transversal à esquerda.

A seguinte proposição nos dá uma condição para sabermos quando $(T, \circ)$ é um loop transversal:

Proposição 2.1.3. *Considere $T = \{x_1 = e, x_2, \ldots\}$ um transversal à direita de H em G com a operação $(\circ)$ definida anteriormente. Então o transversal T relativo ao subgrupo H de G é um loop transversal se, e somente se, T é um transversal para todo conjugado de H.*

Prova:
$(\Rightarrow)$Por hipótese $(T, \circ)$ é um loop transversal. Suponha que $x_i \circ x_j = x_i \circ x_m$. Assim, $x_i x_j = h_1 x_k$ e $x_i x_m = h_2 x_k$ onde $h_1, h_2 \in H$ e $x_k \in T$. Agora, $x_i x_j x_m^{-1} x_i^{-1} = x_i x_j (x_i x_m)^{-1} = h_1 x_k (h_2 x_k)^{-1} = h_1 h_2^{-1}$. Chamando $h = h_1 h_2^{-1}$ temos $x_j x_m^{-1} = x_i^{-1} h x_i$, ou seja, $x_j = x_i^{-1} h x_i x_m$.
Se T não é um transversal à direita para $g^{-1}Hg$, para todo $g \in G$, em particular T não é um transversal à direita relativo a $x_i^{-1}Hx_i$, para todo $x_i \in T$. Porém, se T não é um transversal para $x_i^{-1}Hx_i$ então o cancelamento à esquerda não é possível em $(T, \circ)$, contradizendo o fato de T ser loop transversal. Logo, T é um transversal para todo conjugado de H.

$(\Leftarrow)$ Suponhamos que T seja um transversal à direita para $g^{-1}Hg$, para todo $g \in G$, então o cancelamento à direita vale em $(T, \circ)$. Mas isto é equivalente a T ser um transversal à direita para $x_i^{-1}Hx_i$ para qualquer $x_i \in T$. Então o cancelamento à esquerda é válido em T, e portanto, T é um loop transversal para H. □

Se $(T, \circ)$ é comutativo então o cancelamento à esquerda é automaticamente satisfeito e temos o seguinte corolário:

Corolário 2.1.4. *Nas mesmas condições da proposição anterior, se $(T, \circ)$ é comutativo então T é um loop transversal.*

Prova: Imediata. □

Quando consideramos o subgrupo H normal em G e T um transversal relativo a H então $(T, \circ)$ tem estrutura de loop e é isomorfo ao grupo quociente G/H. Isto será mostrado na proposição seguinte.

Proposição 2.1.5. *Se H for um subgrupo normal de G e T é um transversal à direita para H então são válidas as seguintes afirmações:*

(i) O transversal T é um loop transversal.
(ii) O loop $(T, \circ)$ é isomorfo ao grupo quociente G/H.

Prova: (i) Imediata.
(ii) Seja $T = \{x_1 = e, x_2, \ldots\}$ um transversal à direita de H em G, onde H é um subgrupo normal de G. Defina $\psi : T \longrightarrow G/H$ por $\psi(x_i) = Hx_i$. Iremos mostrar que ψ é um homomorfismo de loops. De fato, sejam $x_i, x_j \in T$. Assim, $\psi(x_i \circ x_j) = \psi(x_i x_j) = Hx_i x_j = Hx_i Hx_j = \psi(x_i)\psi(x_j)$. Portanto, ψ é homomorfismo de loops. Agora, se $\psi(x_i) = \psi(x_j)$ então $Hx_i = Hx_j$, isto é, $x_i x_j^{-1} \in H$. Pela definição da operação $(\circ)$, $x_i \circ x_j^{-1} = e$. Logo, $x_i = x_j$ e ψ é injetora. É fácil ver que ψ é sobrejetora. Portanto, $(T, \circ)$ é isomorfo a G/H. □

Proposição 2.1.6. *Seja T um transversal do grupo G relativo ao subgrupo H. São equivalentes:*
(i) T é um loop transversal à esquerda.
(ii) T é um loop transversal à direita.

Prova: (i)⇒ (ii) Suponhamos que $T = \{x_1 = e, x_2, \ldots\}$ é um loop transversal à esquerda de H em G. Daí,

$$x_i^{-1} x_j \notin gHg^{-1} \tag{2.1.2}$$

para todo $g \in G$ e para todo $x_i \neq x_j$.
Suponhamos que T não é um loop transversal à direita para H. Assim, existem $g_1 \in G$, $x_k, x_w \in T$ tais que $x_k = g_1 h g_1^{-1} x_w$, com $h \in H$ e $x_k \neq x_w$.
Logo, $x_w^{-1} x_k = g_2 h^{-1} g_2^{-1}$, onde $g_2 = x_w^{-1} g_1$, o que contradiz 2.1.2. Portanto, T é um loop transversal à direita de H em G.
A recíproca é análoga. □

A partir de agora, bem como na próxima seção, G será sempre grupo finito. Como vimos na Proposição 2.1.5, se H é normal em G qualquer transversal T é um loop transversal pois $(T, \circ)$ é isomorfo a G/H. Em [1], o Teorema 1.1 mostra que se N é o maior subgrupo normal em G que está contido em H então existe uma correspondência bijetora entre loops transversais de H em G e loops transversais de H/N em G/N, fazendo corresponder loops isomorfos. Assim, a existência de um loop transversal de um subgrupo H de um grupo G pode ser reduzido ao caso onde H não possui subgrupos normais não triviais em G.

Dessa forma, considere H um subgrupo de G tal que H não contém nenhum subgrupo normal não trivial. Sejam C o conjunto de todas as classes laterais à direita de H em G, $C = \{H, Hx_2, \ldots, Hx_n\}$, e $P(C)$ as bijeções de C em C. Observe que, para cada $g \in G$, g pertence à uma única classe lateral Hx_i. Suponha que $T = \{e, x_2, \ldots, x_n\}$ é loop transversal. Então para todo $x_i, x_j \in T$ existe um único $x_k \in T$ tal que $x_i \circ x_j = x_k$. Considere $\pi : G \longrightarrow P(C)$ a representação fiel em classes laterais à direita de H que associa para cada $g \in G$ a função $\pi(g) : C \to C$. Se $g \in H$ então definimos $\pi(g)$ como sendo a função identidade , isto é, $\pi(g)(Hx_i) = Hx_i$, para todo $i = 1, 2, \ldots, n$. Se $g \in G$ tal que $g \notin H$ então $g \in Hx_i$, para um único x_i, e faz sentido considerar a representação π somente nos elementos $\{x_2, \ldots, x_n\}$. Assim, $\pi(x_i) : C \longrightarrow C$ e $\pi(x_i)(Hx_j) = Hx_k$, onde $x_i \circ x_j = x_k$ e $(\circ)$ é a operação em T. Para simplificar a notação utilizaremos apenas $\pi_i(x_j)$ ao invés de $\pi(x_i)(Hx_j)$.

A matriz (a_{ij}), onde $a_{ij} = \pi_i(x_j)$, é um quadrado latino. Neste caso, o quadrado latino é exatamente a tábua de multiplicação do loop correspondente. Portanto, a existência de um loop transversal é equivalente a existência de um subconjunto de permutação $\{\pi_1 = e, \pi_2, \ldots, \pi_n\}$.

2.2 Loops Transversais e Grupos de Permutação

O teorema de Cayley afirma que todo grupo finito é isomorfo à um subgrupo de um grupo de permutações. Nesta seção, consideramos G um grupo finito como sendo um grupo de permutações sobre um conjunto finito Ω e vamos nos restringir no caso em que G é um grupo de permutação transitiva. Fixamos também, G_α como sendo o subgrupo estabilizador do elemento α, $\alpha \in \Omega$.

Proposição 2.2.1. *Sejam G um grupo de permutação transitiva sobre um conjunto finito Ω e $\alpha \in \Omega$. Considere $H = G_\alpha$ e T um transversal relativo a H. Então T é um loop transversal para H.*

Prova: Seja $\gamma \in \Omega$, $\gamma \neq \alpha$. Pela Proposição 1.2.4, existe $g \in G$ tal que $G_\gamma = gHg^{-1}$. Se $T = \{e, x_2, \ldots, x_n\}$ é um transversal para G_γ em G então T será um transversal para todo conjugado gHg^{-1}. Pela Proposição 2.1.3 temos que T é um loop transversal de H em G. □

Nas condições da proposição anterior, se T é um loop transversal para $H = G_\alpha$ então T consiste de elementos que são livres de ponto fixo. De fato, considere $J =$

$\{gHg^{-1}; g \in G\}$ o conjunto de todos os conjugados de H. Pela transitividade da ação todo elemento de J é exatamente o estabilizador de algum ponto $\gamma \in \Omega$, $\gamma \neq \alpha$. Reciprocamente, se $S = G_\beta$, $\beta \in \Omega$, então $S \in J$. Assim, como T é loop transversal para H, T é um transversal para todo conjugado de H. Porém, observe que todo subgrupo de G que não está em J é livre de ponto fixo. Logo, todos os elementos do transversal são livres de ponto fixo. Daí, segue a proposição:

Proposição 2.2.2. *O loop transversal T relativo ao subgrupo $H = G_\alpha$, $\alpha \in \Omega$, consiste de elementos que são livres de ponto fixo.*

A recíproca do resultado acima não é válida em geral. Isto é, um grupo com transversal livre de ponto fixo não necessariamente produz um loop transversal. Vejamos o exemplo a seguir.

Seja $G = A_5$, o grupo alternado com cinco elementos, agindo por translação à direita nas classes laterais de um subgrupo H de ordem 10 isomorfo ao grupo diedral. Neste caso, considere $H = D_5 = \{(1), (25)(34), (12)(35), (12345), (13)(45), (13524), (15432), (14253), (14)(23), (15)(24)\}$ e $T = \{(1), (135), (354), (23)(45), (234), (243)\}$ um transversal à direita de H em G.

Na tábua de Cayley abaixo podemos observar que T não possue estrutura de loop:

$\circ$	(1)	(135)	(354)	(23)(45)	(234)	(243)
(1)	(1)	(135)	(354)	(23)(45)	(234)	(243)
(135)	(135)	**(23)(45)**	(1)	(243)	**(23)(45)**	(354)
(354)	**(354)**	(243)	**(135)**	**(354)**	**(135)**	(23)(45)
(23)(45)	(23)(45)	**(1)**	(234)	**(1)**	(354)	(135)
(234)	**(234)**	(354)	**(243)**	**(234)**	**(243)**	(1)
(243)	(243)	**(234)**	(23)(45)	(135)	(1)	**(234)**

O grupo das translações à direita de um loop qualquer Q é um subgrupo do grupo das permutações nos elementos de Q gerado pelas permutações $\{R(x); x \in Q\}$ definida por: $qR(x) = qx$ para todo $q \in Q$.

Já vimos na Proposição 2.2.1, se G age transitivamente em conjunto finito $\Omega = \{1, 2, \ldots, n\}$ e que se tomarmos como subgrupo H de G o estabilizador de algum ponto $\alpha \in \Omega$, então o transversal T de G relativo ao subgrupo H será um loop

transversal. Convém ainda destacar a recíproca desse fato, que é verdadeira como vemos na próxima proposição.

Proposição 2.2.3. *Todo loop Q pode ser considerado como um loop transversal de algum grupo G por algum subgrupo H.*

Prova: De fato, basta tomar o grupo G como sendo o grupo multiplicativo de Q, e já que G permuta os elementos de Q, podemos considerar H subgrupo de G como o estabilizador de algum elemento $q \in Q$. Nessas condições, G terá um loop transversal T associado à H. Claramente, Q e T são isomorfos via a função $R : Q \longrightarrow T$. Note que, se $R(x) = R(y)$ então $x = eR(x) = eR(y) = y$, para todo $x, y \in Q$. □

Portanto, uma maneira óbvia de obter grupos com loops transversais é calcular o grupo das translações à direita de um loop qualquer.

Um exemplo de uma família de grupos de permutação com loop transversal são os grupos de Frobenius.

Definição 2.2.4. *Um grupo de Frobenius é um grupo de permutação transitiva tal que cada elemento não trivial fixa no máximo um ponto.*

Seja G um grupo que age sobre um conjunto Ω. O núcleo de Frobenius K de G consiste do elemento identidade e de todos os elementos que não fixam nenhum ponto. O núcleo de Frobenius pode não ser um subgrupo de G, uma vez que a operação em K pode não ser fechada.

O subgrupo H de um grupo de Frobenius que fixa um ponto é chamado complemento de Frobenius. Em 1901, Frobenius provou que núcleos de Frobenius para grupos de Frobenius são subgrupos normais. Exceto em casos muito particulares não existe prova do resultado acima sem fazer uso da Teoria de Caracteres. E mais, grupos de Frobenius têm um único núcleo de Frobenius. Portanto, tais grupos tem um único loop transversal T tal que $(T, \circ)$ é um grupo (que na realidade é o núcleo de Frobenius).

Capítulo 3

Anel Centralizador de Grupos de Permutação

Apresentamos neste capítulo alguns tópicos relacionados ao conceito de anel centralizador para grupos de permutação. Uma importante simplificação acontece quando esse é comutativo. Introduzimos a definição de esquema associativo que generaliza o anel centralizador.

3.1 Anel Centralizador

Sejam G um grupo finito de permutação transitiva sobre o conjunto $\Omega = \{1, 2, \ldots, n\}$ e V um espaço vetorial complexo de dimensão finita.

Sejam $\{u_1, u_2, \ldots, u_n\}$ uma base de V e a ação π de G em V que associa para cada $g \in G$ a função $\pi(g) : V \longrightarrow V$ dada por $\pi(g)(u_i) = u_{g(i)}$. Essa é uma representação de permutação cujas matrizes são:

$$[\pi(g)]_{i,j} = \begin{cases} 1, & \text{se, e somente se,} \quad g(i) = j \\ 0, & \text{caso contrário} \end{cases}$$

Consideremos a ação diagonal de G sobre $\Omega \times \Omega$: $g(i, j) = (g(i), g(j))$. Sejam H o estabilizador do 1, denotado por G_1, e $\Delta_0, \Delta_1, \ldots, \Delta_k$ as órbitas da ação de G em $\Omega \times \Omega$.

Definição 3.1.1. *O anel centralizador R de G é o conjunto das matrizes de ordem n (com entradas complexas) que comutam com todas as matrizes $\pi(g)$.*

Para cada órbita Δ_k, seja A_k a *matriz de incidência* $n \times n$ dada por:

$$[A_k]_{i,j} = \begin{cases} 1, & \text{se } (i,j) \in \Delta_k \\ 0, & \text{caso contrário} \end{cases} \tag{3.1.1}$$

Note que se $\mid \Delta_k \mid = t$ então A_k é t - regular, isto é, A_k possui t entradas iguais a 1.

Proposição 3.1.2. *Uma base para o anel centralizador é dada pelo conjunto das matrizes de incidência $A_0, A_1, \ldots, A_k$ de $\Delta_0, \Delta_1, \ldots, \Delta_k$.*

Prova: Seja $B = [B]_{i,j}$ uma matriz complexa arbitraria. Temos que,

$$[\pi(g)B\pi(g)^{-1}]_{i,j} = [B]_{g(i),g(j)}$$

para todo $g \in G$. Assim, $\pi(g)B\pi(g)^{-1} = B$ se, e somente se, $[B]_{i,j} = [B]_{g(i),g(j)}$, para todo $g \in G$.

Iremos mostrar que para todo $g \in G$, $\pi(g)$ comuta com A_r, $r = 0, 1, \ldots, k$. De fato, se $(i,j) \in \Delta_r$, para alguma órbita Δ_r, então a matriz A_r que representa Δ_r tem a (i,j)-ésima posição igual a 1. Logo,

$$[\pi(g)A_r\pi(g)^{-1}]_{i,j} = [A_r]_{g(i),g(j)} = 1.$$

Se $(i,j) \notin \Delta_r$ então $[A_r]_{i,j} = 0$, e portanto,

$$[\pi(g)A_r\pi(g)^{-1}]_{i,j} = [A_r]_{g(i),g(j)} = 0$$

pois como $(i,j) \notin \Delta_r$ então não existe $g \in G$ tal que $(g(i), g(j)) \in \Delta_r$. Assim, em ambos os casos $\pi(g)$ comuta com A_r, para todo $r = 0, 1, \ldots, k$.

Se B comuta com $\pi(g)$, para todo $g \in G$, então $B = \sum_{r=0}^{s} c_r A_r$, com $c_r \in \mathbb{C}$. De fato, inicialmente observemos que o conjunto de todas as órbitas $\Delta_0, \Delta_1, \ldots, \Delta_k$ formam uma partição em $\Omega \times \Omega$ e que (i,j) e (j,i) estão na mesma órbita, e assim, cada matriz de incidência $A_0, A_1, \ldots, A_k$ será simétrica. Além disso, o conjunto $\{A_0, A_1, \ldots, A_k\}$ é linearmente independente. Seja B uma matriz qualquer de ordem n que comuta com as matrizes π_g, para todo $g \in G$. Temos que $[B]_{i,j} = [B]_{g(i),g(j)}$, para todo $g \in G$. Façamos $i = j = 1$. Como g percorre todos os elementos de G, então existe $g \in G$ tal que $g(1) = 1, g(1) = 2, \ldots, g(1) = n$, ou seja, $[B]_{1,1} = [B]_{2,2} = \ldots = [B]_{n,n}$. Logo, a diagonal da matriz B é formada por elementos que são todos iguais. Agora, consideremos $i \neq j$. Como a ação é transitiva, existe $g \in G$ tal que $g(i) = j$ e $g(j) = i$. Assim, $[B]_{i,j} = [B]_{j,i}$, e portanto, B é uma matriz simétrica. Logo,

$B = c_0A_0 + c_1A_1 + \ldots + c_sA_s$, com $c_i \in \mathbb{C}, s = 0, 1, \ldots, k$. Portanto, as matrizes de incidência A_r formam uma base para o anel centralizador. □

Consideremos o grupo finito $G = \{g_1, g_2, \ldots, g_n\}$, onde $g_1 = e$ (o elemento identidade). A cada g_i vamos associar a variável x_{g_i}. Definimos a *matriz grupo* X_G como sendo uma matriz $n \times n$ tal que a (i, j)-ésima entrada é $x_{g_i}x_{g_j^{-1}}$. Assim o anel centralizador pode também ser caracterizado como um conjunto de matrizes que comutam com a matriz grupo $X_G^{\pi} = \sum \pi(g)x_g$ que corresponde a π.

Exemplo: Seja o grupo diedral $D_4 = \{e, g_2 = (1234), g_3 = (1432), g_4 = (13), g_5 = (24), g_6 = (13)(24), g_7 = (12)(34), g_8 = (14)(23)\}$ agindo sobre $\Omega \times \Omega$, onde $\Omega = \{1, 2, 3, 4\}$.
A ação pode ser descrita abaixo:

$$\begin{array}{ccc} D_4 \times (\Omega \times \Omega) & \longrightarrow & \Omega \times \Omega \\ \sigma \times (a, b) & \longmapsto & (\sigma(a), \sigma(b)) \end{array}$$

onde as órbitas dessa ação são:
$\Delta_0 = \{\sigma(1,1); \sigma \in D_4\} = \{(1,1), (2,2), (3,3), (4,4)\}$
$\Delta_1 = \{\sigma(1,3); \sigma \in D_4\} = \{(1,3), (2,4), (4,2), (3,1)\}$
$\Delta_2 = \{\sigma(1,2); \sigma \in D_4\} = \{(1,2), (2,3), (4,1), (3,2), (1,4), (3,4), (2,1), (4,3)\}$

Consideremos V espaço vetorial de dimensão 4 e $B = \{e_1, e_2, e_3, e_4\}$ a base canônica de V. As matrizes de representação de G sobre $\mathbb{C}$ são:

$$\pi(e) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \pi(g_2) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad \pi(g_3) = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\pi(g_4) = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \pi(g_5) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \quad \pi(g_6) = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

$$\pi(g_7) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad \pi(g_8) = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

enquanto as matrizes de incidência são:

$$A_0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad A_1 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \quad A_2 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

O anel centralizador R de D_4 tem como base as matrizes A_0, A_1, A_2. Vejamos a tábua de R, onde $(\cdot)$ é a multiplicação usual de matrizes:

$\cdot$	A_0	A_1	A_2
A_0	A_0	A_1	A_2
A_1	A_1	A_0	A_2
A_2	A_2	A_2	$2A_0 + 2A_1$

3.2 Comutatividade do Anel Centralizador

É interessante sabermos se o anel centralizador de um grupo de permutação G é comutativo (veja [2, 16]). Por exemplo, a comutatividade implica que a representação de permutação de G, que se decompõe em representações irredutíveis, possue a propriedade de que cada representação irredutível aparece no máximo uma vez, como veremos a seguir.

Retornaremos a situação geral do grupo G agindo em um conjunto Ω.

A representação de permutação $g \to \pi(g)$ é claramente uma representação linear sobre $\mathbb{C}$, e portanto, cinde em fatores irredutíveis $\pi = \sum_{i=1}^{s} c_i\sigma_i$, onde σ_i é uma representação irredutível de G. Dizemos que π é *livre de multiplicidade* se cada $c_i = 1$.

Teorema 3.2.1. *Se G age em um conjunto Ω via $g \to \pi(g)$ o anel centralizador é comutativo se, e somente se, π é livre de multiplicidade.*

Prova: Suponhamos que π é livre de multiplicidade. Assim, $\pi = \sum_{i=1}^{s} \sigma_i$. Então a matriz grupo $X_G^{\pi} = \sum \pi(g)x_g$ é similar a matriz bloco,

$$D_\pi = \begin{bmatrix} X_{\sigma_1} & 0 & \cdots & 0 & 0 \\ 0 & X_{\sigma_2} & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & X_{\sigma_s} \end{bmatrix}$$

que corresponde a decomposição de π em representações irredutíveis. Pelo Lema de Schur temos que qualquer matriz que comuta com o a matriz grupo que correspondem a representações irredutíveis é da forma λI, onde λ é um escalar e I é a matriz identidade (consulte [8, Proposição 2.1.3]). Portanto, qualquer matriz que comuta com D_π deve ser diagonal da forma,

$$\begin{bmatrix} \lambda_1 I_{n_1} & 0 & \cdots & 0 & 0 \\ 0 & \lambda_2 I_{n_2} & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & \lambda_s I_{n_s} \end{bmatrix}$$

onde λ_i são escalares arbitrários, $i = 1, 2, \ldots, s$.

Claramente, o anel gerado por essas matrizes diagonais é comutativo. Logo, o anel centralizador é comutativo.

Suponhamos que π não é livre de multiplicidade, isto é, existe $c_i \in \mathbb{C}$ tal que $c_i > 1$. Por outro lado, as matrizes que comutam com a matriz da forma

$$\begin{bmatrix} X_\sigma & 0 \\ 0 & X_\sigma \end{bmatrix}$$

são da forma

$$\begin{bmatrix} \lambda_1 I & \lambda_2 I \\ \lambda_3 I & \lambda_4 I \end{bmatrix}$$

onde $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ são escalares arbitrários. É claro que a álgebra de tais matrizes é isomorfa a álgebra das matrizes 2×2 que não é comutativa. Logo, o anel centralizador não é comutativo. □

No caso onde R é comutativo, o par (G, H) é freqüentemente chamado de *par de Gelfand*.

3.3 Esquemas Associativos

Sejam Ω um conjunto finito não vazio e $R = \{R_0, R_1, \ldots, R_d\}$ uma coleção de subconjuntos de $\Omega \times \Omega$ em $(d+1)$-classes. A forma $\chi = (\Omega, \{R_i\}_{0 \leq i \leq d})$ ou simplesmente χ é chamado um *esquema associativo* de d classes se satisfaz as seguintes propriedades:
(1) $R_0 = \{(x, x); x \in \Omega\}$.
(2) Para quaisquer R_i, o conjunto $R_i^t = \{(x, y); (y, x) \in R_i\}$ pertence a R.
(3) Para todo par $(x, y) \in R_h$, o número de elementos $z \in \Omega$ tal que $(x, z) \in R_i$, $(z, y) \in R_j$ é a constante $p_{i,j}^h$ dependendo somente de h, i, j. As constantes $p_{i,j}^h$ são chamados números de interseção (ou parâmetros) de χ.

Além disso se χ satisfazer a seguinte condição:
(4) $p_{i,j}^h = p_{j,i}^h$, para todo h, i, j.
dizemos que χ é um esquema associativo comutativo. Freqüentemente na literatura o termo esquema associativo inclui a comutatividade.

Definimos a composição de R_i e R_j por:

$$R_i \circ R_j = \{(x, y); \exists z; (x, z) \in R_i, (z, y) \in R_j\}$$

Assim, a condição (3) acima é equivalente a:

$$R_i \circ R_j = p_{i,j}^h R_h$$

ou seja, com a composição definida acima, os elementos de χ formam uma álgebra sobre $\mathbb{Z}$. A condição (4) é equivalente a $R_i \circ R_j = R_j \circ R_i$, em outras palavras, a álgebra descrita acima é comutativa. Além disso, o esquema associativo é chamado simétrico se a seguinte condição é válida:
(5) $R_i = R_i^t$, para todo $i = 0, 1, \ldots, d$.
Note que (5) implica (4).

Observação 3.3.1. *Existem várias definições na literatura para esquemas associativos. Aqui estaremos utilizando a definição onde um esquema associativo satisfaz as condições de (1) a (4) descritas acima.*

Exemplo: Seja G um grupo finito munido de uma operação $(*)$ agindo em si mesmo através de $(*)$. Para cada $g \in G$, considere $R_g = \{(x, y); x = g * y\}$. Assim, (G, R_i)

é esquema associativo. Note que se G é abeliano então o esquema associativo é comutativo.

Cada R_i do esquema associativo é descrito por sua matriz adjacente A_i definida exatamente como em 3.1.1. Em termos das matrizes adjacentes, a definição pode ser reescrita da seguinte maneira:
(1) $A_0 = I$, onde I é a matriz identidade.
(2) $A_i = A_i^T$, para todo $i = 0, 1, \ldots, d$.
(3) $A_i A_j = \sum_k p_{i,j}^k A_k$.

Além disso, $\sum_{i=0}^{d} A_i = J$, onde J é a matriz cujas entradas são todas iguais a 1. Logo, as matrizes A_i são linearmente independentes e pelos itens (1), (2) e (3) vemos que geram uma álgebra comutativa $\mathbf{A}$, $(d+1)$-dimensional. Essa álgebra foi estudada primeiramente por Bose e Mesner (1959) e por isso é conhecida como a álgebra de Bose-Mesner do esquema associativo. As matrizes $A_0, A_1, \ldots, A_d$ formam a chamada base canônica da álgebra de Bose-Mesner. Observe que as matrizes A_i são normais, isto é, comutam com sua transposta conjugada. Pelo Teorema Espectral, como as matrizes A_i comutam, elas podem ser diagonalizadas simultaneamente, isto é, existe uma matriz unitária U tal que para cada $A \in \mathbf{A}$, $U^{-1}AU$ é diagonal (uma matriz U é dita unitária se $U^{-1} = U^T$). Portanto, $\mathbb{C}^n = V_0 \oplus V_1 \oplus \cdots \oplus V_d$, onde cada V_i é um autoespaço de $A_0, A_1, \ldots, A_d$ respectivamente.

Seja E_i a projeção ortogonal $\mathbb{C}^n \to V_i$, expressada na forma de matriz com respeito a base canônica. Então essas matrizes satisfazem:
$(i) \sum_{i=0}^{k} E_i = I$
$(ii) E_i E_j = \delta_{ij} E_i$

Em particular, podemos tomar $E_0 = \frac{1}{n} J$, onde J é a matriz cujas entradas são todas iguais a 1. As matrizes $E_0, E_1, \ldots, E_d$ são uma base de idempotentes ortogonais para $\mathbf{A}$.

Sejam $\{V_0, V_1, \ldots, V_d\}$ o conjunto de autoespaços de $A_0, A_1, \ldots, A_d$ respectivamente e a matriz $X \in R$,

$$X = \alpha_0 A_0 + \alpha_1 A_1 + \ldots + \alpha_d A_d$$

onde $\alpha_i \in \mathbb{C}$, $i = 0, 1, \ldots, d$. Os vetores de V_i são exatamente os autovetores da matriz X e podemos escolher V_0 o subespaço unidimensional com base $\{v_{01} = (1, 1, \ldots, 1)\}$.

Explicitamente, se $\{v_{i1}, v_{i2}, \ldots, v_{is_i}\}$ formam uma base para V_i então uma base para o espaço fundamental V é dada pelos vetores:

$$\{v_{01}, v_{11}, v_{12}, \ldots, v_{1s_1}, \ldots, v_{d_1}, \ldots, v_{ds_d}\}.$$

Com respeito a essa base podemos escrever cada $v \in V$ como: $v = \sum_{j=0}^{d} \sum_{k=1}^{s_j} \alpha_{jk} v_{jk}$.

Assim P_i, a projeção na coordenada i, leva v em $\sum_{k=1}^{s_i} \alpha_{ik} v_{ik}$. Além disso, $A_i = \sum_{j=0}^{d} p_i(j) E_j$ onde $p_i(j)$ são os autovalores de A_i.

Vamos retornar ao exemplo da página 23, onde o grupo diedral D_4 age sobre $\Omega \times \Omega$, com $\Omega = \{1, 2, 3, 4\}$. Note que os autovalores de A_0 são todos iguais a 1 com multiplicidade algébrica 4, os autovalores de A_1 são 1 e -1 ambos com multiplicidade algébrica 2 e os autovalores de A_2 são 2, -2 e 0 com multiplicidade algébrica 2. Seja $X \in R$, $X = \alpha A_0 + \beta A_1 + \gamma A_2$ onde $\alpha, \beta, \gamma \in \mathbb{C}$.

Os autovetores de X são: $v_{01} = (1, 1, 1, 1)$, $v_{11} = (-1, 1, -1, 1)$, $v_{21} = (0, -1, 0, 1)$ e $v_{22} = (-1, 0, 1, 0)$. Assim,
$V_0 =< (1, 1, 1, 1) >$ $\quad$ $V_1 =< (-1, 1, -1, 1) >$ $\quad$ $V_2 =< (0, -1, 0, 1), (-1, 0, 1, 0) >$
e consideramos $V =< V_0, V_1, V_2 >$. Seja $v = (a, b, c, d) \in V$. Então,
$v = \alpha_{01} v_{01} + \alpha_{11} v_{11} + \alpha_{21} v_{21} + \alpha_{22} v_{22}$
$(a, b, c, d) = \alpha_{01}(1, 1, 1, 1) + \alpha_{11}(-1, 1, -1, 1) + \alpha_{21}(0, -1, 0, 1) + \alpha_{22}(-1, 0, 1, 0)$

$$(a, b, c, d) = \frac{a+b+c+d}{4} v_{01} + \frac{b+d-a-c}{4} v_{11} + \frac{d-b}{2} v_{21} + \frac{c-a}{2} v_{22}.$$

Consideremos as projeções:

$$\begin{array}{rccc} P_0 : & V & \longrightarrow & V \\ & v & \longmapsto & \alpha_{01} v_{01} \end{array} \qquad \begin{array}{rccc} P_1 : & V & \longrightarrow & V \\ & v & \longmapsto & \alpha_{11} v_{11} \end{array} \qquad \begin{array}{rccc} P_2 : & V & \longrightarrow & V \\ & v & \longmapsto & \alpha_{21} v_{21} + \alpha_{22} v_{22} \end{array}$$

As matrizes das transformações lineares P_i, $i = 0, 1, 2$, na base canônica são:

$$E_0 = \frac{1}{4} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \quad E_1 = \frac{1}{4} \begin{bmatrix} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \end{bmatrix} \quad E_2 = \frac{1}{2} \begin{bmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix}$$

Observe que E_0, E_1, E_2 são idempotentes e são ortogonais dois a dois.

O esquema associativo generaliza o conceito de anel centralizador de um grupo de permutação, pois todo anel centralizador é um esquema associativo onde as órbitas Δ_i podem ser identificadas com os R_i do esquema associativo. Um esquema associativo que surge através da ação de um grupo em um conjunto é chamado *Schurian*. Frizamos que nem todos os grupos de permutação dão origem a esquemas associativos, já que em geral o anel centralizador pode não ser comutativo.

Capítulo 4

S-Anéis

Nas próximas seções estudamos vários resultados para S-anéis sobre loops equivalentes aos encontrados em [12], que trata a respeito de S-anéis sobre grupos. A passagem de S-anéis sobre grupos para S-anéis sobre loops não é imediata e os conceitos necessários para tal são aqui tratados. Também estabelecemos uma relação entre o S-anel e o anel centralizador que foi definido no capítulo anterior. Todos os resultados explorados neste capítulo a respeito de S-anéis sobre loops podem ser vistos em [6, 7].

4.1 S-Anéis

Primeiramente, começamos definindo S-anel sobre grupos:

Definição 4.1.1. *Sejam H um grupo e $\mathbb{Z}H$ o anel de grupo sobre $\mathbb{Z}$. Um S-anel sobre H é um subanel S de $\mathbb{Z}H$ tal que existe uma partição $H = \cup J_i$, $J_i \neq \emptyset$ satisfazendo:*
(i) $J_0 = \{e\}$
(ii) $J_i^* = J_j$ *para algum* j, *onde* $J_i^* = \{x; x^{-1} \in J_i\}$
(iii) $\{\overline{J_0}, \overline{J_1}, \cdots, \overline{J_n}\}$ *é base para o grupo abeliano livre* $(S, +)$, *onde se* $J_i = \{x_1, x_2, ..., x_r\}$ $\overline{J_i}$ *denota o elemento* $x_1 + x_2 + \cdots + x_r$ *de* $\mathbb{Z}H$.

Um grupo abeliano G é chamado *abeliano livre* se esse é uma soma direta de grupos cíclicos infinitos. Mais precisamente, existe um subconjunto $X \subset G$ de elementos de ordem infinita, chamado *base de* G, com $G = \sum_{x \in X} < x >$.

O S-anel S é *primitivo* se $i > 0$ implica que o grupo gerado por J_i é igual a H e S é dito *primitivo trivial* se existem apenas duas partições de H: $J_0 = \{e\}$ e $J_1 = H - \{e\}$.

Considere um grupo G agindo sobre um subgrupo H por translações à direita. Dizemos que G é primitivo mediante essa ação se G não preserva partição não trivial de H. Seja S o S-anel de H, isto é, $S =< \overline{J_0}, \overline{J_1}, \ldots, \overline{J_n} >$ onde os J_i são como definidos acima. Um resultado interessante nos diz que G é primitivo se, e somente se, S é primitivo. Para maiores detalhes dessa prova consulte [12]. Se ainda, H for um subgrupo regular de G então o anel centralizador R de G é isomorfo ao S-anel sobre H. Veja [16].

No que segue, iremos obter resultados equivalentes aos anteriores quando o grupo H é substituido por um loop $Q = \{q_1 = 1, q_2, ..., q_n\}$ tal que cada elemento de Q possui inverso bilateral.

Lembramos que o conceito de *anel de loop* é o equivalente não associativo dos anéis de grupo, onde o grupo é substituido por um loop qualquer.

Definição 4.1.2. *Um S-anel sobre Q é um subanel de $\mathbb{Z}Q$ com uma partição $Q = \cup J_i$, $J_i \neq \emptyset$ tal que as condições (i), (ii), (iii) anteriores são satisfeitas.*

Um S-anel sobre Q é *primitivo* se $i > 0$ implica que o loop gerado por J_i é Q.

Mostraremos que, se G é um grupo de permutação com um loop transversal T dando origem a um loop Q então o anel centralizador de G sobre $\mathbb{Z}$ é anti-isomorfo ao S-anel sobre Q e que G é primitivo se, e somente se, o S-anel sobre Q é primitivo.

Nos resultados a seguir, iremos assumir que G é um grupo de permutação transitiva em $\{1, 2, ..., n\}$ que contém um loop transversal $T = \{x_1, x_2, ..., x_n\}$ relativo a G_1.

Note que $(T, \circ)$ é isomorfo ao loop Q, onde o isomorfismo $\sigma : T \longrightarrow Q$ é dado por: $\sigma(x_i) = q_i$, para todo $i = 1, 2, ..., n$.

O grupo G age em T via:

$$\begin{array}{rcl} G \times T & \longrightarrow & T \\ (g, x_i) & \longmapsto & x_{g_{(i)}} \end{array}$$

e da mesma maneira em Q:

$$\begin{array}{rcl} G \times Q & \longrightarrow & Q \\ (g, q_i) & \longmapsto & q_{g_{(i)}} \end{array}$$

Agora considere a ação de T sobre Q:

$$\begin{array}{rcl} T \times Q & \longrightarrow & Q \\ (x_j, q_i) & \longmapsto & q_i\sigma(x_j) = q_iq_j. \end{array}$$

O grupo G contém uma cópia isomorfa do grupo das translações à direita de Q via a função $\varphi : R(q_j) \to x_j$, e G será reconhecido como um grupo de permutação nos elementos de Q. Denotamos por e o elemento identidade de Q e por $\overline{G_e}$ a soma dos elementos que pertencem a G_e (estabilizador do elemento neutro de Q).

Proposição 4.1.3. *Se $q \in Q$, $g \in G$, então qg é o único elemento $x \in Q$ tal que $\overline{G_e}R(x) = \overline{G_e}R(q)g$ em $\mathbb{Z}G$.*

Prova: Temos que $\overline{G_e}R(x) = \overline{G_e}R(q)g$ se, e somente se, $G_eR(x) = G_eR(q)g$. Como $eG_eR(qg) = eG_eR(q)g$, segue que $x = qg$. □

Proposição 4.1.4. *Sejam $x = \sum n_iq_i$ em $\mathbb{Z}Q$ e $R(x) = \sum n_iR(q_i) \in \mathbb{Z}G$. Então xg é o único elemento y de $\mathbb{Z}Q$ tal que $\overline{G_e}R(y) = \overline{G_e}R(x)g$.*

Prova: Seja $x = \sum n_iq_i$ em $\mathbb{Z}Q$. Por hipótese, $R(x) = \sum n_iR(q_i) \in \mathbb{Z}G$. Daí, $\overline{G_e}R(xg) = \overline{G_e}\sum n_iR(q_ig)$ e $\overline{G_e}R(x)g = \overline{G_e}\sum n_iR(q_i)g$. Pela Proposição 4.1.3, temos que $\overline{G_e}\sum R(q_ig) = \overline{G_e}\sum R(q_i)g$. Assim, temos a igualdade $\overline{G_e}R(xg) = \overline{G_e}R(x)g$.
Se $\overline{G_e}R(y) = \overline{G_e}R(x)g$ onde $y = \sum m_iq_ig$ então,

$$\overline{G_e}R(y) = \overline{G_e}R(x)g = \overline{G_e}\sum n_iR(q_i)g = \sum n_i\overline{G_e}R(q_i)g.$$

e $R(y) = \sum m_iR(q_ig)$. Logo,

$$\sum m_i\overline{G_e}R(q_ig) = \overline{G_e}\sum m_iR(q_ig) = \overline{G_e}R(y) = \sum n_i\overline{G_e}R(q_i)g.$$

Como os elementos $\overline{G_e}R(q_i)g \in \mathbb{Z}G$ são linearmente independentes, segue que $m_i = n_i$. Portanto, $R(y) = R(xg)$, ou seja, $y = xg$. □

Seja $\mathbb{Z}(Q, G_e)$ o subgrupo aditivo abeliano livre de $\mathbb{Z}Q$ gerado por $\overline{J_0}, ..., \overline{J_m}$ onde $J_0, ..., J_m$ são as órbitas de G_e mediante a ação de G_e em Q. Observe que a função $\beta : Q \longrightarrow G$ tal que $\beta(q) = R(q)$ nos dá uma imersão de Q em G.

Sabemos que, $\mathbb{Z}(Q, G_e) \subset \mathbb{Z}Q$. Seja $u = \sum n_iq_i \in \mathbb{Z}(Q, G_e)$, $R(u) = \sum n_iR(q_i) \in \mathbb{Z}G$. Assim, podemos estender linearmente a função $\beta : \mathbb{Z}(Q, G_e) \longrightarrow \mathbb{Z}G$ por $\beta(u) = R(u)$. Essa imersão obviamente preserva a soma. Mais tarde mostraremos que $\mathbb{Z}(Q, G_e)$ é associativo.

Proposição 4.1.5. *Se $x \in \mathbb{Z}Q$, então $x \in \mathbb{Z}(Q, G_e)$ se, e somente se, $xg = x$ para todo $g \in G_e$.*

Prova: Seja $x = \sum n_i q_i \in \mathbb{Z}Q$.
Se $xg = x$, para todo $g \in G_e$, então quando dois elementos q_1 e q_2 estão numa mesma órbita de G_e eles possuem os mesmos coeficientes em x. Logo, $x = \sum m_i \overline{J_i}$, e assim, $x \in \mathbb{Z}(Q, G_e)$.
Reciprocamente, se $x \in \mathbb{Z}(Q, G_e)$ então $x = \sum m_i \overline{J_i}$ com $m_i \in \mathbb{Z}$. Obviamente, quando dois elementos quaisquer q_1 e q_2 estão em uma mesma órbita de G_e esses possuem o mesmo coeficiente em x. Portanto, $xg = x$ para todo $g \in G_e$. □

Proposição 4.1.6. *Seja $x \in \mathbb{Z}Q$. As seguintes condições são equivalentes:*
(1) $x \in \mathbb{Z}(Q, G_e)$
(2) *Se $u \in G_e$ então $\overline{G_e}R(x)u = \overline{G_e}R(x)$.*
(3) $\overline{G_e}R(x)\overline{G_e} = |G_e|\overline{G_e}R(x)$.

Prova: As equivalências de (1) e (2) seguem diretamente das duas últimas proposições pois, se $x \in \mathbb{Z}Q$ então $x \in \mathbb{Z}(Q, G_e)$ se, e somente se, $xu = x$ para todo $u \in G_e$, o que é equivalente a $\overline{G_e}R(x) = \overline{G_e}R(x)u$.

(2)⇒(3)
Seja $u \in G_e$. Note que, $\overline{G_e}R(x)\overline{G_e} = \sum_{u \in G_e} \overline{G_e}R(x)u$. Por hipótese, $\overline{G_e}R(x)u = \overline{G_e}R(x)$. Portanto, $\overline{G_e}R(x)\overline{G_e} = |G_e|\overline{G_e}R(x)$.

(3)⇒(2)
Se a condição (3) é satisfeita e $u \in G_e$ então, $|G_e|\overline{G_e}R(x)u = \overline{G_e}R(x)\overline{G_e}u = \overline{G_e}R(x)\overline{G_e} = |G_e|\overline{G_e}R(x)$. Logo, $\overline{G_e}R(x)u = \overline{G_e}R(x)$. □

Proposição 4.1.7. *Seja $x \in \mathbb{Z}Q$. Então $x \in \mathbb{Z}(Q, G_e)$ se, e somente se, $\overline{G_e}R(x) = R(x)\overline{G_e}$.*

Prova: (⇒) Seja $x \in \mathbb{Z}(Q, G_e)$. Pela linearidade, podemos supor que $x = \overline{J}$ onde J é uma órbita de G_e. Pela Proposição 4.1.6, $\overline{G_e}R(\overline{J})\overline{G_e} = |G_e|\overline{G_e}R(\overline{J})$. Portanto, temos que

$$G_eR(J) = G_eR(J)G_e \supseteq 1R(J)G_e = R(J)G_e$$

Assim, $R(J)G_e \subseteq G_eR(J)$. Como $R(J) \cap G_e = \{e\}$ então,

$$|R(J)G_e| = |J||G_e| = |G_e||J| = |G_eR(J)|.$$

Logo, $R(J)G_e = G_eR(J)$, e com isso,

$$\overline{G_e}R(x) = \overline{G_e}R(\overline{J}) = R(\overline{J})\overline{G_e} = R(x)\overline{G_e}.$$

($\Leftarrow$) Por hipótese $\overline{G_e}R(x) = R(x)\overline{G_e}$. Portanto, $\overline{G_e}R(x)\overline{G_e} = \overline{G_e}^2R(x) = |G_e|\overline{G_e}R(x)$. Pela Proposição 4.1.6, $x \in \mathbb{Z}(Q, G_e)$. □

Proposição 4.1.8. *Se $x \in \mathbb{Z}(Q, G_e)$, $g \in G$ e $u \in \mathbb{Z}Q$, então $(xu)g = x(ug)$.*

Prova: Se $x, u \in Q$ então $\overline{G_e}R(xu) = \overline{G_e}R(x)R(u)$.
Usando a Proposição 4.1.7 e a Proposição 4.1.4, se $x \in \mathbb{Z}(Q, G_e)$, $u \in \mathbb{Z}Q$ e $g \in G$ então, $\overline{G_e}R(x(ug)) = \overline{G_e}R(x)R(ug) = R(x)\overline{G_e}R(ug) = R(x)\overline{G_e}R(u)g = \overline{G_e}R(x)R(u)g = \overline{G_e}R(xu)g = \overline{G_e}R((xu)g)$. Como $x(ug) \in \mathbb{Z}Q$, temos que $x(ug) = (xu)g$. □

Como já mencionamos anteriormente, estamos assumindo que cada elemento $x \in Q$ possue inverso bilateral x^{-1}. Assim, $R(x^{-1}) = R(x)^{-1}$ para todo $x \in Q$. Utilizaremos esse fato na demonstração da próxima proposição.

Proposição 4.1.9. *O subgrupo aditivo $\mathbb{Z}(Q, G_e)$ de $\mathbb{Z}Q$ é um S-anel sobre Q.*

Prova: A Proposição 4.1.8 e a Proposição 4.1.5 implicam que $\mathbb{Z}(Q, G_e)$ é fechado com relação a multiplicação. Resta mostrar que $\mathbb{Z}(Q, G_e)$ satisfaz a condição (ii) da definição de S-anel.
Sejam $x, y \in J_i$ e $x^{-1} \in J_j$. Então existe $g \in G_e$ tal que $xg = y$. Assim,

$$eR(x)gR(y)^{-1} = xgR(y)^{-1} = yR(y)^{-1} = e.$$

Logo, $R(x)gR(y)^{-1} \in G_e$. Agora,

$$x^{-1}R(x)gR(y)^{-1} = egR(y)^{-1} = eR(y)^{-1} = y^{-1}.$$

Portanto, $y^{-1} \in J_j$, e temos que, $J_j = J_i^*$. □

Proposição 4.1.10. *O grupo G é primitivo se, e somente se, $\mathbb{Z}(Q, G_e)$ é o S-anel primitivo.*

Prova:

($\Rightarrow$) Suponhamos que o S-anel $\mathbb{Z}(Q, G_e)$ não é primitivo. Assim, existe um loop P, $\{e\} < P < Q$, e uma órbita $J \neq \{e\}$ de G_e tal que J gera P. Se P não é a união de órbitas de G_e então existe uma órbita U, um elemento $a \in U \cap P$ e um elemento

$b \in U - P$.
Como J gera P, algum $\overline{J}^m$ contém a e então contém b também (pois $\mathbb{Z}(Q, G_e)$ é um S-anel), e portanto, $b \in P$ o que é um absurdo. Logo, P é a união de órbitas de G_e, e assim, $\overline{P} \in \mathbb{Z}(Q, G_e)$. Pela Proposição 4.1.7, $\overline{G_e}R(\overline{P}) = R(\overline{P})\overline{G_e}$, e consequentemente, $G_eR(P) = R(P)G_e$. Se $g_1, g_2 \in G_e$ e $p_1, p_2 \in P$ então,
$g_1R(p_1)g_2R(p_2) = g_1(R(p_1) \cdot g_2)R(p_2) = g_1(g_3R(p_3))R(p_2)$ (para algum $g_3 \in G_e, p_3 \in P$) $= g_1g_3g_4R(p_3p_2)$ (para algum $g_4 \in G_e$). Logo, $G_eR(P)$ é um subgrupo próprio de G, $G_e < G_eR(P) < G$, ou seja, G não é primitivo.
($\Leftarrow$) Se G não é primitivo então existe L tal que $G_e < L < G$. Portanto, $L = G_eK$, onde $K = \{R(q_1), ..., R(q_t)\}$ com $q_1 = e, q_2, ..., q_t \in Q$. Como $R(q_i)R(q_j) = gR(q_v)$ para algum v, onde $v = 1, 2, \ldots, t$, $g \in G_e$, o conjunto $\{q_1, ..., q_t\}$ forma um subloop de Q. Temos que K é também um transversal à esquerda para G_e em L. Logo, $\overline{G_e}$ $\overline{K} = \overline{K}\ \overline{G_e}$ e $q_1 + ... + q_t \in \mathbb{Z}(Q, G_e)$, que implica que $\mathbb{Z}(Q, G_e)$ não é primitivo. $\square$

4.2 A relação entre S-Anel e Anel Centralizador

No capítulo anterior, o anel centralizador de um grupo de permutação arbitrário G agindo em um conjunto finito Ω tem uma base que consiste de matrizes cujas entradas são zero ou um. Esta base pode ser calculada tomando o anel dos inteiros. Definimos a função $L : Q \longrightarrow G$ que associa para cada $x \in Q$ a função $L(x) : Q \longrightarrow G$ dada por $qL(x) = xq$. Observe que L tem uma extensão natural para $\mathbb{Z}Q$.

O próximo teorema é de fundamental importância pois descreve uma base para o anel centralizador de G sobre $\mathbb{Z}$ em termos das órbitas de G_e.

Teorema 4.2.1. *Seja $\{J_i\}_{i\in I}$ o conjunto das órbitas de G_e. Então $\{L(\overline{J_i})\}_{i\in I}$ é uma base para o anel centralizador de G sobre $\mathbb{Z}$.*

Prova: Seja R o anel centralizador de G sobre $\mathbb{Z}$. Cada elemento de R é uma transformação linear em $\mathbb{Z}Q$, e cada elemento $g \in G$ também pode ser reconhecido como uma transformação linear em $\mathbb{Z}Q$.
Sejam $u \in R$ e $p \in Q$. Se $g \in G$ então $gug^{-1} = u$. Considere $pu = \sum_{r\in Q} \alpha_{p,r}r$, onde $\alpha_{p,r} \in \mathbb{Z}$. Note que, $pu = p(gug^{-1}) = (pg)(ug^{-1}) = (pgu)g^{-1} = (\sum_{r\in Q} \alpha_{pg,r}r)g^{-1} = \sum_{r\in Q} \alpha_{pg,r}rg^{-1} = \sum_{q\in Q} \alpha_{pg,qg}q$. Assim, $\alpha_{pg,qg} = \alpha_{p,q}$ para todo $g \in G$.

Em particular, se $g = R(x)$ e $p = e$ então $\alpha_{e,q} = \alpha_{x,qx}$ para todo $x \in Q$, e com isto, $u = \sum_{q \in Q} \alpha_{e,q} L(q)$.
Agora, seja $u = \sum m_q L(q) \in R$ e $g \in G$. Daí, $eu = \sum m_q q$ e $e(gug^{-1}) = \sum m_q qg^{-1}$.
Logo, $m_q = m_{q,g}$ para $g \in G_e$, isto é, $u = \sum_{i \in I} n_i L(\overline{J_i})$, com $n_i \in \mathbb{Z}$.
Resta mostrar que, se J é uma órbita de G_e então $L(\overline{J}) \in R$. De fato, sejam $g \in G$, $q \in Q$ e $J = \{t_i\}_{i \in I}$. Então,
$q(gL(\overline{J})g^{-1}) = (\sum_{i \in I} t_i(qg))g^{-1} = ((\sum_{i \in I} t_i \tau)q)gg^{-1}$, onde $\tau = R(qg) \cdot g^{-1} \cdot R(q^{-1}) \in G_e$.
Assim, $q(gL(\overline{J})g^{-1}) = (\sum_{i \in I} t_i)q = qL(\overline{J})$. Portanto, $L(\overline{J}) \in R$. □

Teorema 4.2.2. *O S-anel $\mathbb{Z}(Q, G_e)$ é anti-isomorfo ao anel centralizador R de G via a função: $u \to L(u)$.*

Prova: É suficiente mostrar que para qualquer par de elementos $u, v \in \mathbb{Z}(Q, G_e)$, $L(uv) = L(v)L(u)$.
Sejam $u = x_1 + x_2 + ... + x_r$ e $v = y_1 + y_2 + ... + y_t$, onde $x_i, y_j \in Q$. Como $uv \in \mathbb{Z}(Q, G_e)$, então pelo Teorema 4.2.1 temos que $L(uv) \in R$.
Desde que R é um anel, temos que $L(v)L(u) \in R$. Um elemento de R é completamente determinado pela ação em e, já que, $e \sum n_i L(q_i) = \sum n_i q_i$, onde $n_i \in \mathbb{Z}$.
Assim, $L(uv) = L(v)L(u)$ se, e somente se, a ação em e é a mesma. Note que, $eL(x_i y_i) = x_i y_i = eL(y_i)L(x_i)$.
Como $L(uv) = \sum L(x_i y_j)$ e $L(v)L(u) = \sum L(y_j)L(x_i)$, com $i = 1, 2, ..., r$, $j = 1, 2, .., t$, segue que, $L(uv) = \sum L(x_i y_j) = \sum L(y_j)L(x_i) = L(v)L(u)$. □

Esse teorema faz a ligação entre dois importantes conceitos: S-anel e anel centralizador, explicitando a relação entre esses.

Corolário 4.2.3. *(Schur) Se Q é um grupo, então $\mathbb{Z}(Q, G_e)$ é isomorfo a R.*

Prova: Sejam as seguintes funções: $\varphi : \mathbb{Z}(Q, G_e) \longrightarrow \mathbb{Z}(Q, G_e)$ tal que $\varphi(u) = u^{-1}$, para todo $u \in \mathbb{Z}(Q, G_e)$, e $L : \mathbb{Z}(Q, G_e) \longrightarrow R$ que associa a cada elemento $u \in \mathbb{Z}(Q, G_e)$ a função $L(u) \in R$. Iremos mostrar que $L \circ \varphi$ é o isomorfismo procurado. De fato, sejam $u, v \in \mathbb{Z}(Q, G_e)$.
$(L \circ \varphi)(uv) = L(\varphi(uv)) = L((uv)^{-1}) = L(v^{-1}u^{-1})$.
Por outro lado, $(L \circ \varphi)(u)(L \circ \varphi)(v) = L(u^{-1})L(v^{-1})$.

Logo, $(L \circ \varphi)(uv) = (L \circ \varphi)(u)(L \circ \varphi)(v)$. Assim, $L \circ \varphi$ é homomorfismo. É fácil ver que $L \circ \varphi$ é bijeção. □

Corolário 4.2.4. *Se Q é comutativo, então $\mathbb{Z}(Q, G_e)$ é isomorfo a R.*

Prova: É imediato já que nesse caso $\mathbb{Z}(Q, G_e)$ é comutativo. □

Corolário 4.2.5. *O S-anel $\mathbb{Z}(Q, G_e)$ é associativo.*

Prova: Como $\mathbb{Z}(Q, G_e)$ é anti-isomorfo ao anel centralizador e esse é associativo (pois é um anel de transformações lineares), segue que $\mathbb{Z}(Q, G_e)$ é também associativo. □

A proposição seguinte é uma aplicação direta do teorema anterior:

Proposição 4.2.6. *Se G é um grupo de permutação e T é um loop transversal de G tal que $(T, \circ)$ é comutativo, então o anel centralizador de G é comutativo.*

Referências Bibliográficas

[1] R. Baer, *Nets and groups*, I. Trans. Amer. Math. Soc. **46** (1939), 110–141.

[2] P. J. Cameron, *Suborbits in transitive permutation groups*, Mathematical Centre, Amsterdam, 1975.

[3] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Wiley-Interscience Publication, 1988.

[4] E. G. Goodaire, E. Jespers, and C. P. Milies, *Alternative loop rings*, North-Holland Mathematics Studies, Amsterdam, 1996.

[5] D. G. Higman, *Intersection matrices for finite permutation groups*, J. Algebra **6** (1967), 22–42.

[6] K. W. Johnson, *Transversals, s-rings and centralizer rings of groups*, Proceedings Algebra Carbondale **848** (1980), 169–177.

[7] ———, *S-rings over loops, right mapping groups and transversal in permutation groups*, Math. Proc. Cambridge Philos. Soc. **89** (1981), 433–443.

[8] L.H.Rowen, *Ring theory, vol.1*, Pure and Applied Mathematics, Academic Press Inc., 1988.

[9] J. J. Rotman, *An introduction to the group theory*, Springer-Verlag, New York, 1995.

[10] I. Schur, *Neuer beweis eines satzes von w. burnside*, Jahrb. Deutsche Math-Verein. **17** (1908), 171–176.

[11] ———, *Zur theorie der einfach transitiven permutationgruppen*, Sitzungsber. Preuss. Akad. Wiss. (1933), 598–623.

[12] W. R. Scott, *Group theory*, Dover Publications, New York, 1987.

[13] 0. Tamaschke, *Ringtheoretische behandlung einfach transitiven permutationsgruppen*, Math. Z. **73** (1960), 393–408.

[14] ———, *Zut theorie der permutationsgruppen mit regularen untergruppe*, Math. Z. **80** (1963), 328–355; 443–465.

[15] H. Wielandt, *Zur theorie der permutationsgruppen*, Math. Z. **40** (1935), 582–587.

[16] ———, *Finite permutation groups*, Academic Press, New York, London, 1964.