# Anéis de Schur

Samir Assuena

Dissertação apresentada
ao
Instituto de Matemática e Estatística
da
Universidade de São Paulo
para
obtenção do título
de
Mestre em Ciências

Programa: Matemática

Orientador: Prof. Dr. Francisco César Polcino Milies

Durante o desenvolvimento deste trabalho o autor recebeu auxílio financeiro da CAPES

São Paulo, 22 de janeiro de 2009

# Anéis de Schur

Este exemplar corresponde à redação
final da dissertação devidamente corrigida
e defendida por Samir Assuena
e aprovada pela Comissão Julgadora.

Banca Examinadora:

- Prof. Dr. Francisco César Polcino Milies (orientador) IME-USP.
- Prof. Dr. Raul Antonio Ferraz IME-USP.
- Prof. Dr. Guilherme Augusto de La Rocque Leal UFRJ.

# Agradecimentos

Agradeço:

À Deus por ter me dado forças para vencer esta etapa muito importante e por ter me dado o maior presente da minha vida, meu filho, Mateus!!!!

Aos meus pais: João Alberto e Virgínia pelo apoio, pela confiança e por tudo o que fizeram ao longo desta vida por mim e pelos meus irmãos.

À minha avó: Carolina Saraiva Andreguetto simplesmente pela sua existência.

À minha esposa, Elisangela Marana, por todo o amor, carinho, compreensão, brigas e, acima de tudo, pelo apoio e confiança. Dedico este trabalho a ela e ao nosso filho Mateus.

Aos meus irmãos: Jorge e Vinícius e suas respectivas esposas Juliane e Érika por estarem presentes e me apoiando durante toda a minha vida.

À meu sogro e minha sogra: Eliseu Marana e Etelvina Marana por tudo o que fizeram, fazem e farão por mim e pelo meu filho.

À toda minha família: tios, tias, primos e primas.

Aos meus cunhados: Edilson Marana e Edmilson Marana, suas respectivas esposas Monise e Fabiana e meu sobrinho Murilo.

Ao Instituto de Matemática e Estatítica, em particular ao Professor César Polcino Milies pelo brilhante trabalho de orientação, pela paciência e compreensão.

À Universidade Federal de São Carlos em particular toda turma do curso de Matemática dos anos 2000 e 2001 e ao Professor Daniel Vendrúscolo.

Aos amigos brasileiros e latino-americanos do Ime e a todos os amigos da minha vida.

Por fim agradeço aos eternos PRIMITIVOS por todos os churrascos e festas que fizemos!!! Jamais esquecerei!!!! Vocês são muito importantes pra mim!!!

# Resumo

Sejam $H$ um grupo finito e $\mathbb{Q}$ o corpo dos números racionais. Neste trabalho estudamos um tipo especial de subálgebras da álgebra de grupo $\mathbb{Q}H$ chamadas *Anéis de Schur sobre $H$*, ou abreviadamente *$S$-anéis sobre $H$*, e suas principais propriedades.

Abordamos também, no segundo capítulo, os conceitos de grafo e digrafo de Cayley e de CI-grupos e provamos que o grupo aditivo $\mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$ é um CI-grupo.

Posteriormente, no capítulo 3, vemos as principais propriedades dos S-anéis e, em particular, damos outra caracterização de S-anéis. Dados um grupo finito $H$ e um grupo de permutações $G$ em $H$, denotamos por $G_1$ o estabilizador do elemento neutro de $H$. Mostramos que o *Módulo de Transitividade do grupo $G_1$* é um S-anel sobre $H$. Finalizando este capítulo, introduzimos o conceito de S-anel *Schuriano* que desempenha um papel fundamental nesta teoria.

No capítulo seguinte, tratamos de um tipo especial de S-anéis, chamados *$p$-$S$-anéis* e, como teorema principal, mostramos que todo $p$-$S$-anel sobre um $p$-grupo abeliano elementar de posto 3 é Schuriano. Este é um resultado de P. Spiga e Q. Wang, provado em [12], que responde a uma pergunta formulada por M. Muzychuk e M. Hirasaka em [6].

No último capítulo, estudamos os isomorfismos entre S-anéis e suas relações com os digrafos de Cayley.

**Palavras-chave:** S-anéis, $p$-$S$-anéis Schurianos, Grupo abeliano elementar.

# Abstract

Let $H$ be a finite group and $\mathbb{Q}$ the field of rational numbers. In this work, we study a special type of subalgebras of the group algebra $\mathbb{Q}H$ known as *Schur Rings over $H$* or, briefly, *S-rings over $H$*, and their most important properties.

We also study, in the second chapter the concepts of Cayley graphs and digraphs and of CI-groups and prove that the additive group of $\mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$ is a CI-group.

Then, in the Chapter 3, we consider the most important properties of S-rings and we give another characterization of S-rings. Given a finite group $H$ and a group $G$ of permutations of $H$, we denote by $G_1$ the stabilizer of identity element of $H$. We show that the *Transitivity Module of* $G_1$ is an S-ring over $H$. We conclude this chapter defining *Schurian S-rings* which play a fundamental role in this theory.

In the next chapter, we study a special type of S-rings, known as *p-S-rings*, and, as our main result, we prove that every $p$-S-ring over an elementary $p$-abelian group of rank 3 is Schurian. This is a result due to P. Spiga and Q. Wang, proved in [12], which answers a question posed by M. Muzychuk e M. Hirasaka in [6].

In the last chapter, we study isomorphisms among S-rings and their relationship with Cayley digraphs.

**Keywords:** S-rings, Schurian $p$-$S$-rings, Elementary abelian group.

# Introdução

Em 1933, I. Schur mostrou que todo grupo de permutações primitivo que contém um subgrupo cíclico regular de ordem composta é 2-transitivo. Para isto, Schur estudou o chamado *Módulo de Transitividade* de um grupo de permutações $G$ sobre um grupo finito $H$ contendo um subgrupo regular. Tal estrutura algébrica é uma subálgebra especial da álgebra de grupo $\mathbb{Q}H$ de $H$ sobre $\mathbb{Q}$ gerada por elementos da forma $\sum_{t \in T} t$ onde $T$ percorre o conjunto completo das órbitas do grupo $G_1$, o estabilizador do elemento 1 de $H$ (elementos deste tipo são chamados *quantidades simples de* $\mathbb{Q}H$). Geralmente, as subálgebras da álgebra de grupo $\mathbb{Q}H$, que possuem uma base formada por quantidades simples, são chamadas de *anéis de Schur sobre* $H$, ou abreviadamente, *S-anéis sobre* $H$.

Partindo disto, Schur conjecturou que todo S-anel sobre um grupo finito $H$ é determinado por um particular grupo de permutações sobre $H$, ou seja, que todo S-anel é o módulo de transitividade de algum grupo de permutações sobre $H$. No entanto, H.Wielandt mostrou que tal conjectura é falsa, dando os primeiros contra-exemplos em [13].

Como homenagem a Schur, os S-anéis que satisfazem tal propriedade são chamados *Schurianos* e, em 2008, P. Spiga e Q. Wang mostraram que todo $p$-S-anel sobre um grupo abeliano elementar de posto três é Schuriano.

Esta dissertação expõe este último trabalho e os pré-requisitos teóricos para sua compreensão.

# Sumário


**1 Preliminares** **2**

1.1 Grupos de Permutações . . . . . 2

1.2 Anéis de Grupo . . . . . 5

1.3 Grupos Abelianos Elementares . . . . . 7

1.4 Transformações Afins . . . . . 8

**2 Grafos de Cayley** **10**

2.1 Grafos e Digrafos de Cayley . . . . . 11

**3 Anéis de Schur** **19**

3.1 Definição e Exemplos . . . . . 19

3.2 Principais Propriedades . . . . . 25

3.3 S-subanéis e S-anéis quociente . . . . . 32

3.4 O Módulo de transitividade . . . . . 32

**4 p-S-anéis** **38**

4.1 p-S-anéis sobre $Z_p^3$ . . . . . 38

**5 Isomorfismos entre S-anéis** **52**

5.1 Definições e Propriedades . . . . . 52

5.2 S-anéis e Digrafos de Cayley . . . . . 59

# Capítulo 1

# Preliminares

O objetivo deste capítulo é fixar a notação e introduzir os conceitos e resultados que serão necessários no decorrer da dissertação .

## 1.1 Grupos de Permutações

Nesta seção vamos reunir todos conceitos básicos sobre grupos de permutações que serão utilizados neste trabalho. Em particular o Teorema 1.1.1 será importante mais adiante.

Seja X um conjunto qualquer e considere o conjunto
$\mathrm{Sym}(X) = \{f\colon X \longrightarrow X \mid f \text{ bijetora } \}$ munido com a seguinte operação : dadas $f, g$ em $\mathrm{Sym}(X)$ definimos $(fg)(x) = g(f(x))$, para todo $x \in X$. Com esta operação, $\mathrm{Sym}(X)$ forma um grupo chamado de **grupo de permutações em X**. Daqui em diante, escreveremos $x^f$ para denotar a imagem do elemento $x$ pela função $f$.

Seja $G \leqslant \mathrm{Sym}(X)$. Dois elementos $x$ e $y$ de $X$ são ditos **G-equivalentes** se existe uma permutação $\pi$ em $G$ tal que $x^\pi = y$. Facilmente verificamos que esta relação é uma relação de equivalência em $X$. As classes de equivalência são chamadas de *G-órbitas* sendo que a $G$-órbita do elemento $x$ é o conjunto $\{x^\pi \mid \pi \in G\}$. Assim, $X$ é particionado em **G-órbitas**.

O grupo de permutações $G$ diz-se **transitivo** se, dado qualquer par de elementos $x, y$ de $X$, existe uma permutação $\pi$ em $G$ tal que $x^\pi = y$. Logo $G$ é transitivo se e somente se existe exatamente uma $G$-órbita, a saber $X$.

Se $Y$ é um subconjunto não vazio de $X$, o **estabilizador** de $Y$ em $G$, denotado por $\mathrm{St}_G(Y)$, é o conjunto de permutações em $G$ que fixam individualmente cada elemento de $Y$. Um grupo de permutações $G$ diz-se **semi-regular** se $\mathrm{St}_G(x) = G_x = 1$, para todo $x$ em $X$. Um grupo de permutações **regular** é um grupo transitivo e semi-regular.

Seja $G$ um grupo de permutações em $X$. Um subconjunto $Y$ de $X$ diz-se um **bloco**, também se chama de T.I.Set(conjunto de interseção trivial), de $G$ se para cada $g \in G$ a imagem de $Y$ por $g$ ou coincide com $Y$ ou não tem nenhum ponto em comum com $Y$, isto é, $Y \subset X$ é um bloco se $Y^g = Y$ ou $Y^g \cap Y = \emptyset$ para todo $g \in G$. Obviamente, o conjunto $X$, o conjunto vazio $\emptyset$ e os conjuntos $\{\alpha\}$ formados por um único elemento são blocos de $G$ em $X$. Chamamos estes blocos de **blocos triviais**. Agora, um grupo de permutações $G$ transitivo diz-se **imprimitivo** se existe pelo menos um bloco $Y$ de $G$ não trivial. Caso contrário, $G$ diz-se **primitivo**. O próximo teorema nos fornece uma condição necessária e suficiente para um grupo ser imprimitivo.

**Teorema 1.1.1.** *Seja $x$ um elemento qualquer de um conjunto $X$. Um grupo transitivo $G$ em $X$ é imprimitivo se e somente se existe um grupo $H$ tal que $G_x \subsetneqq H \subsetneqq G$.*

**Demonstração.**($\Rightarrow$) Seja $G$ um grupo imprimitivo e $Y$ um bloco não trivial de $G$. Seja ainda $H$ o conjunto dos elementos $f \in G$ tais que $Y = Y^f$. Claramente $H$ é um subgrupo próprio de $G$ pois se $H$ é igual a $G$ então para todo $\alpha \in X$ e $\beta \in Y$ existe $g \in G$ tal que $\alpha = \beta^g \in Y$ o que implica $X = Y$ o que não pode ocorrer.

Sejam $x \in Y$ e $g \in G_x$. Como $Y$ é um bloco e $x^g = x$ temos $Y^g = Y$ logo $G_x \leqslant H$. Como, $|Y| > 1$ temos que existem $y \in Y$ com $y \neq x$ e $f \in G$ tal que $x^f = y$. Portanto $f \in H$ mas $f \notin G_x$ mostrando que $G_x \subsetneqq H$.

($\Leftarrow$) Seja $H$ um grupo tal que $G_x \subsetneqq H \subsetneqq G$. Defina $Y = x^H$. Primeiramente vamos mostrar que $Y$ é um bloco de $G$. Seja $\beta \in Y \cap Y^g$ com $g \in G$. Assim $\beta = x^f = x^{f'g}$ com $f, f' \in H$. Logo $f'gf^{-1} \in G_x \subset H$, isto é, $g \in H$. Vamos mostrar que $Y^g = Y$.

De fato, seja $y \in Y^g$ existe $f \in H$ tal que $y = (x^f)^g = x^{f'}$ com $f' \in H$. Agora dado $\alpha \in Y$ existe $f \in H$ tal que $\alpha = x^f = x^{(fg^{-1})g}$, ou seja, $\alpha \in Y^g$ com isso temos $Y^g = Y$ e segue que $Y$ é um bloco. Como $G_x \subset H$, $Y$ não consiste somente de $x$.

Acabamos de mostrar que $Y^g = Y$ vale somente para $g \in H$. Mas existe um $g \in G$ tal que $Y^g \neq Y$ e portanto $Y \neq X$. Logo $Y$ é um bloco não trivial e $G$ é imprimitivo.■

Um corolário imediato é

**Corolário 1.1.2.** *Seja $x$ um elemento qualquer de um conjunto $X$ com $|X| > 1$. Um grupo $G$ transitivo em $X$ é primitivo se e somente se $G_x$ é um subgrupo maximal de $G$.*

**Definição 1.1.3.** *Seja $F \leqslant$ Sym(X) um grupo de permutações arbitrário e* Sup(F)=$\{G \leqslant \mathrm{Sym}(X) \mid F \leqslant G\}$. *Dizemos que $G \in$ Sup$(F)$ é* **F-transjugado** *se para cada $g \in \mathrm{Sym}(X)$ a inclusão $g^{-1}Fg \leqslant G$ implica que $g^{-1}Fg$ e $F$ são conjugados em $G$.*

Dois grupos de permutações são ditos 2-*equivalentes* se eles possuem o mesmo conjunto de 2-órbitas, isto é, órbitas em pares ordenados. Desta forma, dado $G \in$ Sym(X) definimos o 2-*fecho de* $G$ como sendo o conjunto de todas as permutações $h$ em X que preservam 2-órbitas, isto é, todas as permutações que satisfazem: para cada $x, y \in X$ existe $g \in G$ tal que $x^g = x^h, y^g = y^h$. Tal conjunto é um subgrupo de Sym(X) denotado por $G^{(2)}$. Neste caso, se $G = G^{(2)}$ então $G$ diz-se **2-fechado**.

O 2-fecho possui as seguintes propriedades que são facilmente verificadas:

$$G_1 \leqslant G_2 \Rightarrow G_1^{(2)} \leqslant G_2^{(2)}$$

$$(G^{(2)})^{(2)} = G^{(2)}$$

$$G \leqslant G^{(2)}$$

Seja $H$ um grupo arbitrário. Denotamos por $R_x \in \mathrm{Sym}(H)$ a seguinte permutação $h^{R_x} = hx$. Assim, definimos $R_H = \{R_x \mid x \in H\}$.

## 1.2 Anéis de Grupo

Sejam $R$ um anel e $G$ um grupo. Definiremos um novo conjunto e, usando as operações em $R$ e $G$, mostraremos que tal conjunto é um anel. Denotamos por $RG$ o conjunto de todas as combinações lineares da forma

$$\alpha = \sum_{g \in G} a_g g$$

onde $a_g \in R$ e somente um número finito de coeficientes $a_g$ é diferente de zero. Neste sentido, todas as somas podem ser consideradas finitas mesmo quando os índices do somatório percorrem um conjunto infinito.

**Definição 1.2.1.** *Seja $\alpha = \sum_{g \in G} a_g g$ um elemento de $RG$. Definimos o* **suporte** *de $\alpha$ como sendo o conjunto dos elementos $g \in G$ tal que $a_g \neq 0$ em $\alpha = \sum_{g \in G} a_g g$. Mais formalmente,*

$$supp(\alpha) = \{g \in G \mid a_g \neq 0\} \tag{1.1}$$

Observe que, de acordo com a definição , dois elementos $\alpha = \sum_{g \in G} a_g g$ e $\beta = \sum_{g \in G} b_g g$ pertencentes a $RG$ são iguais se e somente se $a_g = b_g$ para todo $g \in G$.

Dados dois elementos $\alpha = \sum_{g \in G} a_g g$ e $\beta = \sum_{g \in G} b_g g$ pertencentes a $RG$, definimos a soma de $\alpha$ e $\beta$ da seguinte maneira:

$$\alpha + \beta = \left(\sum_{g \in G} a_g g\right) + \left(\sum_{g \in G} b_g g\right) = \sum_{g \in G} (a_g + b_g) g \tag{1.2}$$

Agora, dados $\alpha = \sum_{g \in G} a_g g$ e $\beta = \sum_{g \in G} b_g g \in RG$ definimos o produto de $\alpha$ e $\beta$ da seguinte maneira:

$$\alpha\beta = \sum_{g,h \in G} a_g b_h gh \tag{1.3}$$

Verifica-se facilmente que o conjunto $RG$ munido das operações de soma e produto definidas em (1.2) e (1.3) é um anel com unidade. Além disso, podemos definir uma multiplicação de elementos de $RG$ por elementos de $R$ de tal forma que $RG$ seja um $R$-módulo e, se $R$ for um anel comutativo, $RG$ seja uma $R$-álgebra. Tal multiplicação é definida por

$$\lambda\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G}(\lambda a_g)g \tag{1.4}$$

Agora, se $R$ é um anel comutativo, segue diretamente do fato de que $RG$ é um anel e um $R$-módulo que $RG$ é uma $R$-álgebra.

**Definição 1.2.2.** *O conjunto $RG$, com as operações definidas acima, é chamado* **anel de grupo de $G$ sobre $R$.** *Se $R$ é comutativo, $RG$ é também chamado de* **álgebra de grupo de $G$ sobre $R$.**

Considere a função $i : G \to RG$ definida por $i(x) = \sum_{g\in G} a_g g$ onde $a_x = 1$ e $a_g = 0$ se $g \neq x$. Tal função é uma imersão de $G$ em $RG$; portanto, podemos considerar $G$ como um subconjunto de $RG$ e dizer que $G$ é uma base de $RG$ sobre $R$.

Por outro lado, a função $\nu : R \to RG$ dada por $\nu(r) = \sum_{g\in G} a_g g$ onde $a_{1_G} = r$ e $a_g = 0$ se $g \neq 1_G$ é um monomorfismo de anéis. Logo $R$ pode ser considerado como um subanel de $RG$.

Finalizaremos esta seção mostrando que anéis de grupo sobre anéis comutativos são anéis com involução .

**Proposição 1.2.3.** *Seja $R$ um anel comutativo. A aplicação $^*: RG \longrightarrow RG$ definida por*

$$\left(\sum_{g\in G} a_g g\right)^* = \sum_{g\in G} a_g g^{-1}$$

*satisfaz as seguintes propriedades*

*(i)* $(\alpha+\beta)^* = \alpha^* + \beta^*$,

*(ii)* $(\alpha\beta)^* = \beta^*\alpha^*$, *e*

*(iii)* $\alpha^{**} = \alpha$.

A demonstração é elementar por isso vamos omití-la.

## 1.3 Grupos Abelianos Elementares

**Definição 1.3.1.** *Seja $p$ um número primo. Um grupo finito $G$ diz-se um $p$-***grupo** *se sua ordem é uma potência de $p$. Um $p$-grupo abeliano $G$ diz-se* **abeliano elementar** *se todo elemento não trivial tem ordem $p$.*

**Lema 1.3.2.** *Seja $G$ um $p$-grupo abeliano elementar. Então, $G$ é um espaço vetorial sobre $\mathbb{Z}_p$. Além disto, se $G$ é finito então $G$ pode ser ecrito como produto direto de um número finito de grupos cíclicos de ordem $p$.*

**Demonstração.** Denote por $\bar{k}$ a classe de congruência do inteiro $k$ em $\mathbb{Z}_p$. Dado $g \in G$ definimos

$$\bar{k}\cdot g = kg$$

onde $kg = \underbrace{gg\cdots g}_{k \text{ vezes}}$ se $k$ é positivo. Esta operação está bem definida pois se $k \equiv k'(\text{mod}p)$ então $k - k' = mp$ para algum inteiro $m$ logo

$$(k - k')g = (mp)g = 1_G$$

assim

$$kg = k'g.$$

Podemos verificar facilmente que $G$, com as operações ,

$$\begin{aligned} "+": G \times G &\longrightarrow G \\ (g, h) &\longmapsto g + h = gh \end{aligned} \qquad \begin{aligned} ".": \mathbb{Z}_p \times G &\longrightarrow G \\ (\bar{k}, g) &\longmapsto \bar{k} \cdot g = kg \end{aligned}$$

é um espaço vetorial sobre $\mathbb{Z}_p$. Seja $\{g_1, g_2, \ldots, g_t\}$ uma base de $G$ no caso em que $G$ é finito. Neste caso, $G$ é o produto direto dos grupos $\langle g_i \rangle$. ■

Como consequência temos que se $G$ é um $p$-grupo abeliano elementar finito com base $\{g_1, g_2, \ldots, g_t\}$ então $G \simeq \underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{t \text{ vezes}}$. Além disso, se $\varphi\colon G \longrightarrow G$ é um homomorfismo de grupos então $\varphi$ é uma transformação $\mathbb{Z}_p$-linear. De fato, $\varphi(\bar{k} \cdot g) = \varphi(kg) = k\varphi(g) = \bar{k} \cdot \varphi(g)$ para todo $g \in G$ e para todo $\bar{k} \in \mathbb{Z}_p$.

## 1.4 Transformações Afins

Nesta seção vamos explorar o conceito de transformação afim mas antes precisamos da seguinte

**Definição 1.4.1.** *Sejam $H$ e $K$ subgrupos de um grupo $G$. Dizemos que $G$ é um* **produto semi-direto** *de $H$ e $K$, e escrevemos $G = H \rtimes K$, se*

*i)* $G = HK = KH$

*ii)* $H \cap K = \{1_G\}$

*iii)* $H \triangleleft G$

Note que as condições *(i)* e *(ii)* nos dizem que todo elemento $g \in G$ pode ser escrito de maneira única como o produto de um elemento de $H$ por um elemento de $K$. O fato de $K$ não ser necessariamente normal tem consequência no modo como serão multiplicados os elementos de $G$. Dados $k_1h_1, k_2h_2 \in G$ temos:

$$(k_1h_1)(k_2h_2) = k_1k_2k_2^{-1}h_1k_2h_2 = k_1k_2(h_1^{k_2}h_2)$$

**Definição 1.4.2.** *Seja $V$ um espaço vetorial sobre um corpo $\mathbb{F}$. Denote por $GL(V)$ o grupo das transformações lineares de $V$ em $V$ invertíveis. Uma* **transformação afim** *em $V$ é uma função $\alpha$ de $V$ em $V$ tal que existem $T \in GL(V)$ e $a \in V$ para os quais $x^\alpha = x^T + a$ para todo $x \in V$. Uma* **translação** *é uma tal função $\alpha$ para a qual $x^\alpha = x + a$ para todo $x \in V$*

Com isso temos o seguinte

**Teorema 1.4.3.** *Se $V$ é um espaço vetorial sobre um corpo $\mathbb{F}$ então*

*i) o conjunto $G$ das transformações afins forma um grupo,*

*ii) o conjunto das translações forma um subgrupo normal $H$ de $G$,*

*iii) $G = H \rtimes GL(V)$.*

Uma demonstração deste resultado pode ser encontrada em [11].

# Capítulo 2

# Grafos de Cayley

Neste capítulo vamos explorar os Grafos de Cayley mas iniciaremos dando a definição geral de grafos.

**Definição 2.0.4.** *Um* **grafo X** *consiste de um conjunto de vértices V(X) e um conjunto de arestas E(X), onde uma aresta é par não ordenado de vértices distintos de* $X$. *Dados* $x, y \in V(X)$ *vamos usar* $xy$ *para denotar uma aresta. Se* $xy$ *é uma aresta, dizemos que* $x$ *e* $y$ *são adjacentes e denotamos isto por* $x \sim y$.

**Definição 2.0.5.** *Um* **digrafo X** *consiste de um conjunto de vértices V(X) e um conjunto de arcos A(X) onde um arco é um par ordenado de vértices distintos. Um digrafo é um grafo no qual cada aresta tem uma* **orientação** *ou* **direção** *atribuída.*

Note que o conceito de digrafo coincide com a noção de **quivers** usada na Teoria de Representações , onde os arcos são chamados de flechas.

**Definição 2.0.6.** *Dois grafos* $X$ *e* $Y$ *são* **isomorfos** *se existe uma bijeção* $\varphi\colon V(X) \longrightarrow V(Y)$ *tal que* $x \sim y$ *em* $X$ *se e somente se* $\varphi(x) \sim \varphi(y)$ *em* $Y$. *Dizemos que* $\varphi$ *é um* **isomorfismo** *de* $X$ *em* $Y$ *e escrevemos* $X \cong Y$.

## 2.1 Grafos e Digrafos de Cayley

Vamos introduzir aqui alguns grafos e digrafos associados a grupos.

**Definição 2.1.1.** *Seja $H$ um grupo finito e $S \subset H$ um subconjunto de $H$ tal que:*

*(i)* $1 \notin S$

*(ii)* $x \in S \Rightarrow x^{-1} \in S$

*Chama-se* **grafo de Cayley de H sobre S** *ao grafo cujo conjunto de vértices é $H$ e o conjunto de arestas é $\{gh : hg^{-1} \in S\}$*

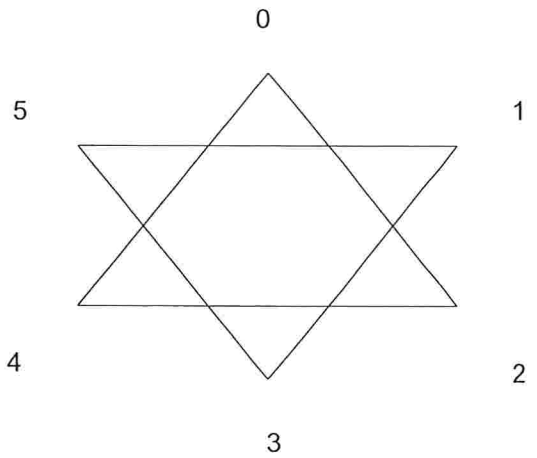


Figura 2.1: Grafo de Cayley do grupo $\mathbb{Z}_6$ sobre $S = \{\bar{2}, \bar{4}\}$

Note que a condição *(i)* implica que um grafo de Cayley não contém *loops*, isto é, arestas da forma $xx$. Por outro lado, como as arestas são não orientadas temos que se $xy$ é uma aresta, isto é, $yx^{-1} \in S$ então $yx$ é a mesma aresta, donde deve-se ter que $xy^{-1} \in S$. Esta é a razão de se impor a condição *(ii)* em $S$.

**Definição 2.1.2.** *Seja $S \subset H$ um subconjunto qualquer de $H$. Chama-se* **digrafo de Cayley de H sobre S** *ao digrafo cujo conjunto de vértices é $H$ e conjunto de arcos $\{(g, h) : hg^{-1} \in S\}$. Assim sendo, $S$ é chamado de* **conjunto de conexão**.

Veremos que a noção de digrafo de Cayley pode-se formalizar também de outra maneira.

Dado $S \subseteq H$ definimos a relação $\mathrm{Cay}(H, S) \subset H \times H$ por:

$$\mathrm{Cay}(H, S)=\{(x, y) \in H \times H \mid xy^{-1} \in S\}$$

Note que

$$(x, y) \in \mathrm{Cay}(H, S) \Leftrightarrow xy^{-1} \in S$$

Denotaremos este fato escrevendo $x \sim y$. Como todo ponto do digrafo de Cayley pertence a algum arco pois, dado $x \in H$ e $s \in S$ arbitrário, o elemento $y = sx$ é tal que $(x, y)$ é um arco, podemos descrever então o digrafo de Cayley pelo seu conjunto de arcos e este pode ser identificado com a relação $\mathrm{Cay}(H, S)$.

**Teorema 2.1.3.** *Sejam $H$ um grupo finito e $S$ um subconjunto de $H$. Então a relação binária $\mathrm{Cay}(H, S)$ é uma relação de equivalência se e somente se $S$ é um subgrupo de $H$.*

**Demonstração.**($\Rightarrow$) Suponhamos que $\mathrm{Cay}(H, S)$ é uma relação de equivalência. Assim $1_H$ pertence a $S$ pois $x \sim x$. Se $x$ pertence a $S$ então $x \sim 1$. Mas isto implica que $1 \sim x$ donde $x^{-1}$ pertence a $S$ para todo $x$ em $S$. Por fim, dados $x, y$ em $S$, sabemos que $x \sim 1$ e $1 \sim y^{-1}$ portanto $x \sim y^{-1}$, em outra palavras $xy$ pertence a $S$ o que nos diz que $S$ é um subgrupo de $H$.

($\Leftarrow$) Suponhamos que $S$ é um subgrupo de $H$. Vamos mostrar que $\mathrm{Cay}(H, S)$ é uma relação de equivalência sobre $H$. De fato:

- Reflexiva: dado $x \in H$ então $x \sim x$ pois $1 \in S$.
- Simétrica: dados $x, y \in H$ se $x \sim y$ temos $xy^{-1} \in S$ mas $S$ é um subgrupo de $H$ logo $(xy^{-1})^{-1} = yx^{-1} \in S$ portanto $y \sim x$.
- Transitiva: dados $x, y, z \in H$ se $x \sim y$ e $y \sim z$ temos $xy^{-1}, yz^{-1} \in S$. Novamente pelo fato de $S$ ser um subgrupo de $H$, $(xy^{-1})(yz^{-1}) = xz^{-1} \in S$ logo $x \sim z$. ■

**Definição 2.1.4.** *Seja $H$ um grupo finito, $S$ e $T$ subconjuntos quaisquer de $H$. Diz-se que* $\mathrm{Cay}(H,S)$ *é* **isomorfo** *a* $\mathrm{Cay}(H,T)$ *e escrevemos* $\mathrm{Cay}(H,S) \cong \mathrm{Cay}(H,T)$ *se existe uma permutação $f$ de $H$ tal que* $\mathrm{Cay}(H,S)^f = \mathrm{Cay}(H,T)$ *onde*
$\mathrm{Cay}(H,S)^f = \{(x^f, y^f), (x,y) \in \mathrm{Cay}(H,S)\}$.

*Dizemos que* $\mathrm{Cay}(H,S)$ *e* $\mathrm{Cay}(H,T)$ *são* **Cayley isomorfos** *se existe um automorfismo $\varphi$ de $H$ tal que $S^\varphi = T$. Note que* $\mathrm{Cay}(H,S)$ *é isomorfo a* $\mathrm{Cay}(H,T)$ *no sentido da* Definição 2.0.6.

A implicação contrária não é verdadeira: dois digrafos de Cayley sobre o mesmo grupo podem ser isomorfos mas não Cayley isomorfos. Dar um exemplo nesse sentido não é simples, mas o leitor achará um em [1].

**Definição 2.1.5.** *Um subconjunto $S \subseteq H$ é dito* **CI-subconjunto** *se para cada $T \subseteq H$ os digrafos* $\mathrm{Cay}(H,S)$, $\mathrm{Cay}(H,T)$ *são isomorfos se e somente se são Cayley isomorfos, isto é, eles são isomorfos se e somente se existe $\varphi \in \mathrm{Aut}(H)$ tal que $S^\varphi = T$. Um grupo $H$ diz-se um* **CI-grupo** *se cada subconjunto de $H$ é um CI-subconjunto.*

Vamos provar que o grupo $\mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$ é um CI-grupo. Para isso, precisamos de alguns conceitos.

**Definição 2.1.6.** *Sejam $H$ um grupo e $S$ um subconjunto qualquer de $H$. Considere o digrafo de Cayley* $\mathrm{Cay}(H,S)$. *Dados $x,y$ em $H$, um* **caminho** *de comprimento* r *em* $\mathrm{Cay}(H,S)$ *de $x$ em $y$ é uma sequência de $r+1$ vértices distintos começando em $x$ e terminando em $y$ tal que vértices consecutivos são adjacentes. Se existe um caminho entre quaisquer dos elementos de $H$ dizemos que* $\mathrm{Cay}(H,S)$ *é* **conexo**. *Caso contrário,* $\mathrm{Cay}(H,S)$ *é* **desconexo**.

**Definição 2.1.7.** *Sejam $H$ um grupo e $S$ um subconjunto qualquer de $H$. O digrafo de Cayley ,*$\mathrm{Cay}(H,S)$, *diz-se* **bipartido** *se $H$ pode ser particionado em dois subconjuntos disjuntos $V_1$ e $V_2$ tal que todo arco é formado por um elemento de $V_1$ e um elemento de $V_2$.*

**Exemplo 2.1.8.** Seja $\mathbb{F}_2$ o corpo finito com dois elementos. Considere o grupo $H = \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$. Para um conjunto de geradores $S$ de $H$, tem-se que o grafo de Cayley, $\mathrm{Cay}(H, S)$, de $H$ sobre $S$ é dado pela Figura 2.3. Definindo $V_1 = \{g_1, g_3, g_5, g_7\}$ e $V_2 = \{g_2, g_4, g_6, g_8\}$ temos que $\mathrm{Cay}(H, S)$ é um grafo bipartido.

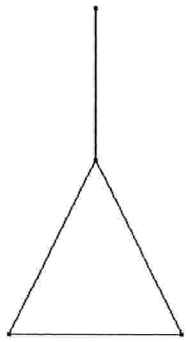

Figura 2.2: Grafo não bipartido

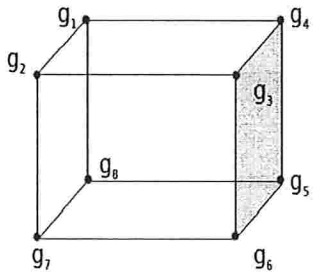


Figura 2.3: Grafo bipartido

**Lema 2.1.9.** *Sejam $H$ um grupo e $S$ um subconjunto qualquer de $H$. O digrafo de Cayley ,Cay(H,S), é conexo se e somente se $S$ é um conjunto de geradores de $H$.*

**Demonstração.** Seja $S$ um subconjunto qualquer de $H$. Suponhamos que $\mathrm{Cay}(H, S)$ é um digrafo conexo. Por hipótese, para quaisquer dois elementos $x, y$ de $H$ existe um caminho de $x$ em $y$. Em particular, tomando $y = 1$, existe um caminho, digamos, de comprimento $r$ de $x$ em 1, ou seja, existem $x = x_1, \ldots, x_{r+1} = 1$ elementos distintos de $H$ tais que os elementos $x_i$ e $x_{i+1}$ são adjacentes.

Com isso, existem $s_1, \ldots, s_r$ elementos de $S$ tais que $x_i x_{i+1}^{-1} = s_i$ para todo índice $i, 1 \leqslant i \leqslant r$. Substituindo as expressões de cada elemento $x_i$ concluímos que $x = s_1 s_2 \ldots s_r$. Mostramos que todo elemento $x$ de $H$ pode ser escrito como produto de elementos de $S$ o que nos diz que $S$ é um conjunto de geradores de $H$.

Reciprocamente, suponhamos que $S$ é um conjunto de geradores de $H$. Dados $x, y$ elementos arbitrários de $H$ precisamos mostrar que existe um caminho de $x$ em $y$. De

fato, o elemento $t = xy^{-1}$ pertence a $H$ e como $S$ é um conjunto de geradores de $H$, existem $s_1, \ldots, s_r$ elementos de $S$ tais que $t = s_1 \ldots s_r$. Logo $x = s_1 \ldots s_r y$.

Defina $t_0 = x$, $t_1 = s_2 s_3 \ldots s_r y$, $t_2 = s_3 s_4 \ldots s_r y$, $\ldots, t_n = y$. Note que

$$t_i t_{i+1} = (s_{i+1} s_{i+2} \ldots s_r y)(y^{-1} s_r^{-1} \ldots s_{i+2}^{-1}) = s_{i+1} \in S$$

Portanto temos uma sequência de vértices de $\mathrm{Cay}(H, S)$ começando em $x$ e terminando em $y$ onde os vértices consecutivos são adjacentes mostrando que $\mathrm{Cay}(H, S)$ é um digrafo conexo. ■

**Lema 2.1.10.** *Seja $S = \{x, y, z, t\}$ um subconjunto de quatro elementos de $H = \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$ tal que $\{x, y, z\}$ é uma base de $H$ sobre $\mathbb{F}_2$. Então :*

*(i) Se $t = xyz$ então $\mathrm{Cay}(H, S)$ é bipartido*

*(ii) Se $t$ é o produto de dois elementos de $\{x, y, z\}$ então $\mathrm{Cay}(H, S)$ não é bipartido*

**Demonstração.** *(i)* Suponhamos que $t = xyz$. Pondo $S = V_1 = \{x, y, z, xyz\}$ e $V_2 = \{1, xy, xz, yz\}$ temos que cada arco de $\mathrm{Cay}(H, S)$ é definido por um vértice de $V_1$ e um vértice de $V_2$. Um cálculo direto mostra que não podemos ter arcos definidos por dois vértices que estão em $V_1$. Mais ainda, $xy(xz)^{-1} = yz \notin S$ e $xy(yz)^{-1} = xz \notin S$. Procedendo de maneira análoga, mostramos que não podemos ter arcos definidos por dois vértices pertencentes a $V_2$ logo $\mathrm{Cay}(H, S)$ é um digrafo bipartido.

*(ii)* Suponhamos que $t$ é o produto de dois elementos de $\{x, y, z\}$. Digamos que $S = \{x, y, z, xy\}$ e suponha que existem conjuntos $V_1$ e $V_2$ disjuntos tais que cada arco de $\mathrm{Cay}(H, S)$ tem um vértice em $V_1$ e outro em $V_2$. Se $x$ e $y$ estão no mesmo conjunto digamos em $V_1$ então o arco $(x, y)$ tem dois vértices do mesmo conjunto.

Logo, podemos supor que $x \in V_1$ e $y \in V_2$. Suponhamos ainda que $1 \in V_1$ (o caso $1 \in V_2$ é análogo). Então $x1^{-1} = x \in S$ é um arco com vértices no mesmo conjunto o que é uma contradição. Portanto $\mathrm{Cay}(H, S)$ não é bipartido. ■

A demonstração elementar do próximo teorema nos foi comunicada verbalmente pelo Professor M.M. Parmenter.

**Teorema 2.1.11.** *O grupo $\mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$ é um CI-grupo.*

**Demonstração.** Sejam $S$ e $T$ subconjuntos de $H = \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$. Pelo Lema 1.3.2, sabemos que $H$ é um espaço vetorial sobre $\mathbb{F}_2$. Suponhamos que $\mathrm{Cay}(H, S) \cong \mathrm{Cay}(H, T)$ e que $1 \notin S$ e $1 \notin T$. Notemos, inicialmente que $|S| = |T|$ pois a cardinalidade do conjunto de arcos de $\mathrm{Cay}(H, S)$ é igual a cardinalidade do conjunto de arcos de $\mathrm{Cay}(H, T)$. Além disto, dado $y \in H$, $x \sim y \Leftrightarrow xy^{-1} \in S \Leftrightarrow x \in Sy$. Assim o número de arcos em $\mathrm{Cay}(H, S)$ é $|S||H|$. Analogamente, mostra-se que o número de arcos em $\mathrm{Cay}(H, T)$ é $|T||H|$ mas $|S||H| = |T||H|$ logo $|S| = |T|$.

Agora, afirmamos que

$$\mathrm{Cay}(H, S) \cong \mathrm{Cay}(H, T) \Leftrightarrow \mathrm{Cay}(H, H - \{1\} - \{S\}) \cong \mathrm{Cay}(H, H - \{1\} - \{T\})$$

De fato, existe uma permutação $\varphi$ em $H$ tal que $\mathrm{Cay}(H, S)^{\varphi} = \mathrm{Cay}(H, T)$ se e somente se dizer que $xy^{-1} \in S$ é igual a dizer que $x^{\varphi}(y^{\varphi})^{-1} \in T$. Portanto $xy^{-1} \notin S$ se e somente se $x^{\varphi}(y^{\varphi})^{-1} \notin T$ o que é equivalente a dizer que
$\mathrm{Cay}(H, H - \{1\} - \{S\})^{\varphi} = \mathrm{Cay}(H, H - \{1\} - \{T\})$.
Pela afirmação acima, é suficiente provarmos o teorema para $|S| \leqslant 4$ pois como $|H| = 8$ se $|S| \geqslant 5$ então $|H \setminus \{S\}| \leqslant 3$.

- **Caso 1:** $|S| = |T| = 1$ ou $|S| = |T| = 2$

  Como $H$ é um espaço vetorial sobre $\mathbb{F}_2$ de dimensão 3, em ambos os casos $S$ e $T$ são conjuntos linearmente independentes. Estendendo-os a bases $S'$ e $T'$ de $H$ respectivamente, definimos uma bijeção $f\colon S' \longrightarrow T'$ de forma tal que: se $x \in S$ então $x^f \in T$ e se $x \notin S$ então $x^f \notin T$. Esta função se estende por linearidade a uma função $\bar{f} \in \mathrm{GL}(H)$ que é um isomorfismo entre $S$ e $T$.

- **Caso 2:** $|S| = |T| = 3$

  Se $S$ e $T$ são linearmente independentes, como dimensão de $H$ sobre $\mathbb{F}_2$ é 3, $S$ e $T$ são bases de $H$ sobre $\mathbb{F}_2$. Assim definimos uma bijeção $f$ que leva cada elemento de $S$ em um elemento de $T$ que se estende a um automorfismo de $H$ que leva $S$ em $T$.

Se $S$ e $T$ são ambos linearmente dependentes então são da forma $S = \{x, y, xy\}$ e $T = \{a, b, ab\}$ para convenientes $x, y, a, b$ em $H$. Definimos a função $f\colon S \longrightarrow T$ por $x^f = a, y^f = b, (xy)^f = ab$ e usando o mesmo argumento do Caso 1, mostra-se que existe um um automorfismo de $H$ que leva $S$ em $T$.

Finalmente, se $S$ é linearmente independente e $T$ é linearmente dependente, pelo Lema 2.1.9, $\mathrm{Cay}(H, S)$ é conexo enquanto que $\mathrm{Cay}(H, T)$ é desconexo o que não pode ser pois $\mathrm{Cay}(H, S) \cong \mathrm{Cay}(H, T)$. O caso contrário ($S$ é linearmente dependente e $T$ é linearmente independente) é análogo.

- **Caso 3:** $|S| = |T| = 4$

  Neste caso, $S$ e $T$ devem conter uma base de $H$ sobre $\mathbb{F}_2$. Digamos que a base contida em $S$ é $\{x, y, z\}$. O quarto elemento de $S$ deve ser um produto de dois ou três elementos de $\{x, y, z\}$. Se este elemento é produto de três elementos, pelo Lema 2.0.6 temos que $\mathrm{Cay}(H, S)$ é um digrafo bipartido. Por outro lado, se este outro elemento é o produto de dois elementos de $S$ então , pelo Lema 2.0.6, $\mathrm{Cay}(H, S)$ não é bipartido.

  Como $\mathrm{Cay}(H, S) \cong \mathrm{Cay}(H, T)$, então $\mathrm{Cay}(H, S)$ é um digrafo bipartido se e somente se $\mathrm{Cay}(H, T)$ também o é. Consequentemente, o quarto elemento de $T$ é um produto dos outros três elementos no caso em que $\mathrm{Cay}(H, T)$ é bipartido ou é o produto de dois elementos no caso em que $\mathrm{Cay}(H, T)$ não é bipartido. Definimos uma função $f$ que leva os elementos da base de $H$ contida em $S$ nos elementos da base de $H$ contida em $T$. Esta função se estende por linearidade a um isomorfismo entre $S$ em $T$. ■

O grupo de automorfismos de um digrafo de Cayley $\mathrm{Cay}(H, S)$, que será denotado por $\mathrm{Aut}(\mathrm{Cay}(H, S))$, consiste de todas as permutações $f \in \mathrm{Sym}(H)$ que satisfazem $\mathrm{Cay}(H, S)^f = \mathrm{Cay}(H, S)$.

**Proposição 2.1.12.** *O conjunto $R_H$ das multiplicações à direita é um subgrupo regular de* $\mathrm{Aut}(\mathrm{Cay}(H,S))$.

**Demonstração.** Seja $h \in H$ e considere $R_h \in R_H$. Vamos mostrar que $\mathrm{Cay}(H,S)^{R_h}$=$\mathrm{Cay}(H,S)$. Seja $(x,y) \in \mathrm{Cay}(H,S)$, assim $xy^{-1} \in S$. Como $R_h \in \mathrm{Sym}(H)$ existem $r,s \in H$ tais que $r^{R_h} = x$ e $s^{R_h} = y$. Mas $rs^{-1} = (xh^{-1})(yh^{-1})^{-1} = xy^{-1} \in S$, ou seja, $(x,y) = (r^{R_h}, s^{R_h})$ com $(r,s) \in \mathrm{Cay}(H,S)$, logo $(x,y) \in \mathrm{Cay}(H,S)^{R_h}$. Agora, se $(x,y) \in \mathrm{Cay}(H,S)^{R_h}$, $(x,y) = (r^{R_h}, s^{R_h})$ para algum $(r,s) \in \mathrm{Cay}(H,S)$. Além disso, $r^{R_h}(s^{R_h})^{-1} = (rh)(sh)^{-1} = rs^{-1} \in S$ portanto $(x,y) \in \mathrm{Cay}(H,S)$. Podemos concluir que $R_H \subset \mathrm{Aut}(\mathrm{Cay}(H,S))$.

Considere a seguinte função

$$\begin{aligned} \psi : H &\longrightarrow \mathrm{Aut}(\mathrm{Cay}(H,S)) \\ h &\longmapsto R_h \end{aligned}$$

Claramente, $\psi$ é um monomorfismo de grupos. Vamos mostrar que $R_H$ é regular. Dados $x,y \in H$ considere $R_{x^{-1}y} \in R_H$. Assim $R_{x^{-1}y}(x) = x(x^{-1}y) = y$ isto nos mostra que $R_H$ é transitivo. Além disso, se existe $h \in H$ tal que $R_h(x) = x$ para algum $x \in H$ então $h = 1$, ou seja, $R_h = Id_H$ portanto $R_H$ é semiregular e, consequentemente, $R_H$ é regular. ■

Esta Proposição mostra que $\mathrm{Aut}(\mathrm{Cay}(H,S))$ contém um subgrupo regular isomorfo à $H$.

Os autores Hirasaka e Muzychuk em [6] provaram que o grupo $\mathbb{F}_p \times \mathbb{F}_p \times \mathbb{F}_p \times \mathbb{F}_p$ é um CI-grupo e Muzychuk em [7] mostrou que se $n \geqslant 2p - 1 + \binom{2p-1}{p}$ então $\underbrace{\mathbb{F}_p \times \ldots \times \mathbb{F}_p}_{n \text{ vezes}}$ não é um CI-grupo.

O estudo destas questões levantou um outro problema relacionado com o grupo $H = \mathbb{F}_p \times \mathbb{F}_p \times \mathbb{F}_p$. Dedicamos o resto desta dissertação a explicitar e responder esta questão .

# Capítulo 3

# Anéis de Schur

## 3.1 Definição e Exemplos

Seja $H$ um grupo finito e considere a álgebra de grupo de $H$ sobre $\mathbb{Q}$ denotada por $\mathbb{Q}H$. Dados dois elementos $\sum_{h\in H} \alpha_h h$, $\sum_{h\in H} \beta_h h \in \mathbb{Q}H$ definimos o *produto de Schur-Hadamard* destes elementos da seguinte forma:

$$(\sum_{h\in H} \alpha_h h) \circ (\sum_{h\in H} \beta_h h) = \sum_{h\in H} (\alpha_h \beta_h) h. \tag{3.1}$$

**Proposição 3.1.1.** *O produto de Schur-Hadamard definido acima é associativo, comutativo e distributivo com relação à adição.*

A demonstração desta proposição é trivial por isso vamos omití-la.

**Definição 3.1.2.** *Para cada subconjunto $T \subseteq H$ definimos $\widehat{T} = \sum_{t\in T} t$. Os elementos desta forma são chamados de* **quantidades simples** *de $\mathbb{Q}H$. Note que as quantidades simples são elementos de $\mathbb{Q}H$ cujos coeficientes são iguais a 0 ou 1.*

Se $x, y$ são dois elementos de $\mathbb{Q}H$ então $\theta_h(x, y)$ denota o coeficiente de $h \in H$ no produto $xy$. Se X,Y são subconjuntos de $H$, então escrevemos $\theta_h(X, Y)$ para $\theta_h(\widehat{X}, \widehat{Y})$.

**Lema 3.1.3.** *$\theta_h(\widehat{X},\widehat{Y}) = |X \cap hY^{(-1)}|$, onde $Y^{(-1)} = \{y^{-1} \mid y \in Y\}$.*

**Demonstração.** Dados $X, Y \subseteq H$, temos que $\widehat{X}\widehat{Y} = \sum_{x\in X}\sum_{y\in Y} xy$ logo $\theta_h(\widehat{X},\widehat{Y})$ é igual ao número de parcelas que $xy = h$, isto é, $\theta_h(\widehat{X},\widehat{Y})$ é o número de elementos $x \in X$ tais $x = hy^{-1}$ portanto $\theta_h(\widehat{X},\widehat{Y}) = |X \cap hY^{(-1)}|$. ■

Vamos agora definir a estrutura que dá nome a este capítulo.

**Definição 3.1.4.** *Uma subálgebra $\mathcal{A}$ da álgebra de grupo $\mathbb{Q}H$ diz-se um* **anel de Schur sobre H**, *abreviadamente* **S-anel sobre H**, *se satisfaz os seguintes axiomas:*

*(S1) $\mathcal{A}$ possui uma base formada por quantidades simples $\widehat{T_0},\ldots,\widehat{T_d}$ onde $T_0 = \{1\}$;*

*(S2) $T_i \cap T_j = \emptyset$ se $i \neq j$ e $\bigcup_{j=0}^{d} T_j = H$;*

*(S3) Para cada $i, 0 \leqslant i \leqslant d$, existe $i', 0 \leqslant i' \leqslant d$, tal que $T_{i'} = T_i^{(-1)} = \{t^{-1} \mid t \in T_i\}$.*

**Proposição 3.1.5.** *Seja $\mathcal{A}$ um S-anel sobre um grupo finito H. A base de $\mathcal{A}$, $\{\widehat{T_0},\ldots,\widehat{T_d}\}$, é a única base de $\mathcal{A}$ formada por quantidades simples de $\mathbb{Q}H$.*

**Demonstração.** Suponhamos que existem subconjuntos $S_0,\ldots,S_d$ de $H$ tais que $\{\widehat{S_0},\ldots,\widehat{S_d}\}$ é uma base de $\mathcal{A}$. Suponhamos ainda que $S_i \cap S_j = \emptyset$ se $i \neq j$ e $\bigcup_{j=0}^{d} S_j = H$.

Devemos mostrar que dado um índice $i, 1 \leqslant i \leqslant d$, existe um único índice $j$, $1 \leqslant j \leqslant d$ tal que $S_j = T_i$. Equivalentemente, dado um índice $i, 1 \leqslant i \leqslant d$, existe um único índice $j, 1 \leqslant j \leqslant d$ tal que $\widehat{S_j} = \widehat{T_i}$.

De fato, suponhamos por absurdo que dado um conjunto básico $T_i$ de $\mathcal{A}$ existem $S_{j_1},\ldots,S_{j_t}$ tais que $\widehat{T_i} = \widehat{S_{j_1}} + \ldots + \widehat{S_{j_t}}$. Nestas condições cada $S_{j_k}$ é um subconjunto próprio de $T_i$. Por outro lado, como $\widehat{S_{j_k}} \in \mathcal{A}$ podemos escrevê-lo como soma de conjuntos básicos de $\mathcal{A}$, digamos $\widehat{S_{j_k}} = \widehat{T_{i_1}} + \ldots + \widehat{T_{i_t}}$. Mas $S_{j_k} \subset T_i$ para todo $k, 1 \leqslant k \leqslant t$ portanto $T_i = T_{i_l}$ para algum índice $l, 1 \leqslant l \leqslant t$, o que implica que $S_{j_k} = T_i$ para todo $k, 1 \leqslant k \leqslant t$. Portanto $\widehat{T_i} = k\widehat{T_i}$ uma contradição. Logo existe um único $S_j$ tal que $S_j = T_i$. ■

A base de $\mathcal{A}$ formada por quantidades simples é chamada de **base padrão de $\mathcal{A}$**. Os conjuntos $T_i, 0 \leqslant i \leqslant d$, são chamados **conjuntos básicos de $\mathcal{A}$** e denotamos por Bsets($\mathcal{A}$)= $\{T_i \mid 0 \leqslant i \leqslant d\}$. A notação $\mathcal{A} = \langle \widehat{T_0}, \ldots, \widehat{T_d} \rangle$ indicará que $\mathcal{A}$ é um S-anel sobre $H$ com conjuntos básicos $\{T_0, \ldots, T_d\}$.

**Proposição 3.1.6.** *Seja $\{T_0 = \{1\}, \ldots, T_d\}$ uma partição de um grupo finito $H$ que satisfaz a condição (S3) da* Definição 3.1.4. *Então o subespaço vetorial de $\mathbb{Q}H$ gerado pelos elementos $\{\widehat{T_0}, \ldots, \widehat{T_d}\}$, denotado por $\langle \widehat{T_0}, \ldots, \widehat{T_d} \rangle$, é um S-anel se e somente se satisfaz a seguinte condição*

*(S4) Para cada tripla i,j,k o número $\theta_t(\widehat{T_i}, \widehat{T_j})$ não depende da escolha de $t \in T_k$.*

**Demonstração.**($\Rightarrow$) Suponhamos que $\mathcal{A} = \langle \widehat{T_0}, \ldots, \widehat{T_d} \rangle$ é um S-anel. Para cada par de índices $i, j$ temos que $\widehat{T_i}\widehat{T_j} \in \mathcal{A}$ portanto é da forma $\widehat{T_i}\widehat{T_j} = \sum_{k=0}^{d} \alpha_k \widehat{T_k}$, ou seja, para todo $t \in T_k, \theta_t(\widehat{T_i}, \widehat{T_j}) = \alpha_k$.

($\Leftarrow$) Dados $i, j$ escrevemos $\widehat{T_i}\widehat{T_j} = \sum_{h \in H} \alpha_h h \in \mathbb{Q}H$. Pela hipótese, se para algum $t \in T_k$ tivermos $\alpha_t \neq 0$ tem-se que $\alpha_h = \alpha_t$ para todo $h \in T_k$.

Isto implica que $\widehat{T_k}$ aparece no produto $\widehat{T_i}\widehat{T_j}$ com coeficiente $\alpha_t = \alpha_k$. Portanto $\widehat{T_i}\widehat{T_j} = \sum_{k=0}^{d} \alpha_k \widehat{T_k} \in \langle \widehat{T_0}, \ldots, \widehat{T_d} \rangle$. Podemos concluir que $\langle \widehat{T_0}, \ldots, \widehat{T_d} \rangle$ é uma subálgebra de $\mathbb{Q}H$ gerada por $\{\widehat{T_0}, \ldots, \widehat{T_d}\}$. Vamos provar que eles são linearmente independentes.

Suponhamos que $\sum_{i=0}^{d} r_i \widehat{T_i} = 0$. Reescrevendo a equação , $\sum_{i=0}^{d} r_i \sum_{t \in T_i} t = 0$ e como os elementos $\widehat{T_i}$'s têm suportes disjuntos e os elementos de $H$ são linearmente independentes sobre $\mathbb{Q}$, segue que $r_i = 0, 0 \leqslant i \leqslant d$. Logo $\{\widehat{T_0}, \ldots, \widehat{T_d}\}$ é um conjunto linearmente independente. ■

A álgebra de grupo $\mathbb{Q}H$ contém dois S-anéis triviais $\langle 1, \widehat{H \setminus \{1\}} \rangle$ e $\mathbb{Q}H$. O próximo teorema nos fornece mais um exemplo de S-anel mas antes precisamos de alguns conceitos.

Seja $H$ um grupo finito. Dados $x$ e $y$ em $H$ dizemos que $x$ é conjugado a $y$ se $y = g^{-1}xg$ para algum $g \in H$.

Esta relação é uma relação de eqüivalência sobre $H$, a classe de eqüivalência de $g$ é chamada *classe de conjugação* e a função $\varphi_g\colon H \longrightarrow H$ definida como $\varphi_g(x) = g^{-1}xg$ é um automorfismo de $H$ que preserva classe de conjugação , isto é, se $T$ é a classe de conjugação do elemento $x$ então $T^{\varphi_g} = T$. Tais propriedades são facilmente verificadas.

**Teorema 3.1.7.** *Seja $H$ um grupo finito e considere a álgebra de grupo $\mathbb{Q}H$. Então o centro $\mathcal{Z}(\mathbb{Q}H)$ de $\mathbb{Q}H$ é um S-anel.*

**Demonstração.** Seja $\{T_i\}_{i=0}^{d}$ o conjunto de todas as classes de conjugação de $H$. Vamos mostrar que $\mathcal{Z}(\mathbb{Q}H)= \langle \widehat{T_0}, \ldots, \widehat{T_d}\rangle$, isto é, que $\mathcal{Z}(\mathbb{Q}H)$ é um S-anel e Bsets($\mathcal{Z}(\mathbb{Q}H)$)=$\{T_0 = 1, \ldots, T_d\}$. Primeiramente, dado $g \in H$ temos $g^{-1}\widehat{T_i}g = g^{-1}(\sum_{t\in T_i} t)g = \sum_{t\in T_i} g^{-1}tg$. Mas, como observado acima, $\sum_{t\in T_i} g^{-1}tg = \sum_{y\in T_i} y = \widehat{T_i}$, ou seja, $g^{-1}\widehat{T_i}g = \widehat{T_i}$. Assim $g\widehat{T_i} = \widehat{T_i}g$ para todo $g \in H$ mostrando que $\widehat{T_i} \in \mathcal{Z}(\mathbb{Q}H)$ para todo índice $i, 0 \leqslant i \leqslant d$.

Suponhamos que $\sum_{i=0}^{d} r_i\widehat{T_i} = 0$. Reescrevendo a equação , $\sum_{i=0}^{d} r_i \sum_{t\in T_i} t = 0$ e como os elementos $\widehat{T_i}$'s têm suportes disjuntos e os elementos de $H$ são linearmente independentes sobre $\mathbb{Q}$, segue que $r_i = 0, 0 \leqslant i \leqslant d$. Logo $\{\widehat{T_0}, \ldots, \widehat{T_d}\}$ é um conjunto linearmente independente.

Agora, dado $\alpha = \sum_{g\in H} a_g g \in \mathcal{Z}(\mathbb{Q}H)$, seja $h = x^{-1}gx$ para algum $x \in H$. Então $\alpha = x^{-1}\alpha x$ pois $\alpha$ é central. Equivalentemente, $\sum_{g\in H} a_g g = \sum_{g\in H} a_g x^{-1}gx$. Comparando o coeficiente de $h$ em ambos lados desta equação, podemos concluir que $a_h = a_g$. Isto mostra que todo elemento $h$ pertencente a classe de conjugação de $g$ também pertence a $supp(\alpha)$ e $a_h = a_g$. Portanto $\alpha = \sum_{i=0}^{d} a_i\widehat{T_i}$. Em outras palavras, o conjunto $\{\widehat{T_0}, \ldots, \widehat{T_d}\}$ gera $\mathcal{Z}(\mathbb{Q}H)$.

Por fim, seja $T_i$ a classe de $g$. Dado $y \in T_i$ existe $x \in H$ tal que $y = x^{-1}gx$ logo $y^{-1} = x^{-1}g^{-1}x$, isto é, $y \sim g$ se e somente se $y^{-1} \sim g^{-1}$. Isto implica que para cada $i, 0 \leqslant i \leqslant d$, existe $i', 0 \leqslant i' \leqslant d$, tal que $T_{i'} = T_i^{(-1)}$ o que completa a demonstração

do teorema. ■

A seguir vamos apresentar uma outra caracterização de S-anéis e para isto precisamos de alguns resultados.

**Definição 3.1.8.** *Um anel $R$ diz-se* **semi-simples** *se $R$ é uma soma direta de um número finito de ideais minimais à esquerda. Um elemento $e \in R$ diz-se* **idempotente** *se $e^2 = e$.*

O seguinte teorema é bem conhecido. Veja por exemplo [9].

**Teorema 3.1.9.** *Seja $R = \bigoplus_{i=1}^{t} L_i$ uma decomposição de um anel semi-simples como soma direta de ideais minimais à esquerda. Então existe uma família $\{e_1, \ldots, e_t\}$ de elementos de $R$ tal que:*

*i)* $e_i \neq 0$ *é um idempotente,* $1 \leqslant i \leqslant t$

*ii) Se* $i \neq j$ *então* $e_i e_j = 0$

*iii)* $1 = e_1 + \cdots + e_t$

*iv)* $e_i$ *não pode ser escrito como* $e_i = e_i' + e_i''$ *onde* $e_i', e_i''$ *são idempotentes tais que* $e_i', e_i'' \neq 0$ *e* $e_i' e_i'' = 0, 1 \leqslant i \leqslant t$.

**Definição 3.1.10.** *Seja $R$ um anel, uma família de idempotentes $\{e_1, \ldots, e_t\}$ satisfazendo as condições (i), (ii) e (iii) do teorema acima é chamada* **família completa de idempotentes ortogonais**. *Um idempotente diz-se* **primitivo** *se satisfaz a condição (iv) do teorema acima.*

Agora vamos lembrar um resultado clássico da teoria de álgebras de grupo. Veja, por exemplo, [9].

**Teorema 3.1.11** (Maschke). *Sejam $G$ um grupo finito e $\mathbb{F}$ um corpo. Então $\mathbb{F}G$ é semi-simples se e somente se $car(\mathbb{F}) \nmid |G|$, onde $car(\mathbb{F})$ é a característica de $\mathbb{F}$.*

**Teorema 3.1.12** (Caracterização de S-anéis). *Seja $\mathcal{A} \subseteq \mathbb{Q}H$ uma subálgebra da álgebra de grupo $\mathbb{Q}H$. Então $\mathcal{A}$ é um S-anel sobre $H$ se e somente se $1_H \in \mathcal{A}$, $\widehat{H} \in \mathcal{A}$ e $\mathcal{A}$ é fechada com respeito ao produto de Schur-Hadamard e a involução usual de $\mathbb{Q}H$.*

**Demonstração.** Suponhamos que $\mathcal{A}$ é um S-anel e seja $\mathrm{Bsets}(\mathcal{A}) = \{T_0, \ldots, T_d\}$ onde $T_0 = \{1_H\}$. Assim $1_H \in \mathcal{A}$ e $\bigcup_{j=0}^{d} T_j = H$. Mas isto implica que $\widehat{H} = \sum_{k=0}^{d} \widehat{T_k}$ portanto $\widehat{H} \in \mathcal{A}$.

Agora, dados quaisquer elementos $\alpha, \beta \in \mathcal{A}$ existem $\alpha_1, \ldots, \alpha_d$ e $\beta_1, \ldots, \beta_d$ pertencentes a $\mathbb{Q}$ tais que $\alpha = \sum_{s=0}^{d} \alpha_s \widehat{T_s}$ e $\beta = \sum_{s=0}^{d} \beta_s \widehat{T_s}$. Assim

$$\alpha \circ \beta = \Big(\sum_{s=0}^{d} \alpha_s \widehat{T_s}\Big) \circ \Big(\sum_{s=0}^{d} \beta_s \widehat{T_s}\Big) = \sum_{s=0}^{d} (\alpha_s \beta_s) \widehat{T_s} \in \mathcal{A}$$

e

$$\alpha^* = \sum_{s=0}^{d} \alpha_s (\widehat{T_s})^* = \sum_{s=0}^{d} \alpha_s \widehat{T_s^{(-1)}} \in \mathcal{A}.$$

Reciprocamente, suponhamos que $1_H \in \mathcal{A}$, $\widehat{H} \in \mathcal{A}$ e $\mathcal{A}$ seja fechada para " $\circ$ " e para a involução usual de $\mathbb{Q}H$. Queremos mostrar que $\mathcal{A}$ satisfaz as condições da Definição 3.1.4. Vamos considerar $\mathbb{Q}H$ como uma álgebra com respeito ao produto de Schur-Hadamard. Claramente $\mathbb{Q}H$, com esta estrutura é isomorfa à $\underbrace{\mathbb{Q} \oplus \cdots \oplus \mathbb{Q}}_{|H| \text{ vezes}}$ e, assim, é comutativa e semi-simples.

Sabe-se que uma álgebra de dimensão finita é semi-simples se e somente se seu radical de Jacobson é zero. Como $\mathcal{A}$ tem dimensão finita e é comutativa, seu radical de Jacobson, $J(\mathcal{A})$, é nilpotente. Por outro lado, $\underbrace{\mathbb{Q} \oplus \cdots \oplus \mathbb{Q}}_{|H| \text{ vezes}}$ não contém elementos nilpotentes não nulos logo $J(\mathcal{A}) = 0$. Portanto, $\mathcal{A}$ é comutativa e semi-simples com respeito ao produto de Schur-Hadamard. Pelo Teorema 3.1.9, $\mathcal{A}$ tem uma base de idempotentes primitivos(em relação a este produto), digamos $x_1, \ldots, x_d$. Mas note que se $x = \sum_{g \in H} a_g g$ é um desses idempotentes então $a_g = 0$ ou $1$ para todo $g \in H$. Logo $x_i = \widehat{T_i}$ onde $T_i = supp(x_i) \subset H$. Além disso, sabemos que $x_i \circ x_j = 0$ se $i \neq j$, o que implica $T_i \cap T_j = \emptyset$, de fato se existe $t \in T_i \cap T_j$ então $t \in supp(\widehat{T_i} \circ \widehat{T_j})$ o que é absurdo.

Assim provamos que $\mathcal{A}$ satisfaz as condições *(S1)* e *(S2)* da Definição 3.1.4. Para provar a condição *(S3)* note que a aplicação $x \longrightarrow x^*$ é um automorfismo da álgebra $(\mathcal{A}, \circ)$, portanto $x_i = \widehat{T_i}$ é um $\circ$-idempotente primitivo se e somente se $\widehat{T_i}^* = \widehat{T_i^{(-1)}}$ também o é. Concluímos que $T_i^{(-1)} = T_{i'}$ para algum $i', 0 \leqslant i' \leqslant d$. ■

Uma consequência imediata deste Teorema é o seguinte

**Corolário 3.1.13.** *Seja $H$ um grupo finito. Então a interseção de S-anéis sobre $H$ é um S-anel sobre $H$.*

## 3.2 Principais Propriedades

**Definição 3.2.1.** *Seja $H$ um grupo finito e $\mathcal{A}$ um S-anel sobre $H$. Um subconjunto(subgrupo) $X \subseteq H$ diz-se um* **$\mathcal{A}$-subconjunto(*$\mathcal{A}$*-subgrupo)** *se $\widehat{X} \in \mathcal{A}$.*

**Proposição 3.2.2.** *Seja $H$ um grupo finito e $\mathcal{A}$ um S-anel sobre $H$. Um subconjunto(subgrupo) $X \subseteq H$ é um $\mathcal{A}$-subconjunto(subgrupo) se e somente se $X$ é uma união de conjuntos básicos de $\mathcal{A}$.*

**Demonstração.** Inicialmente, considere $\mathrm{Bsets}(\mathcal{A}) = \{T_0, \ldots, T_d\}$. Se $X \subseteq H$ é tal que $\widehat{X} \in \mathcal{A}$ existem $\alpha_1, \ldots, \alpha_d \in \mathbb{Q}$ não todos nulos e $\widehat{X} = \sum_{i=0}^{d} \alpha_i \widehat{T_i}$. Note que se $\alpha_i \neq 0$ então $\alpha_i = 1$ pois dado $x \in X$ o coeficiente de $x$ em $\widehat{X}$ é 1 logo o coeficiente de $x$ em $\sum_{i=0}^{d} \alpha_i \widehat{T_i}$ deve ser 1. Assim $\widehat{X} = \sum_{j=0}^{t} \widehat{T_{i_j}}$ o que nos mostra que $X = \bigcup_{j=0}^{t} T_{i_j}$ onde $T_{i_j} \in \mathrm{Bsets}(\mathcal{A})$. Por outro lado se $X = \bigcup_{j=0}^{t} T_{i_j}$ onde $T_{i_j} \in \mathrm{Bsets}(\mathcal{A})$, então $\widehat{X} = \sum_{j=0}^{t} \widehat{T_{i_j}} \in \mathcal{A}$. ■

Dados $x_1, \ldots, x_k$ elementos de $\mathbb{Q}H$, definimos $\langle\langle x_1, \ldots, x_k \rangle\rangle$ como sendo o menor S-anel que contém $x_1, \ldots, x_k$ cuja existência é garantida pelo Corolário 3.1.13. Dado $q \in \mathbb{Q}$ e $\alpha = \sum_{g \in H} a_g g \in \mathbb{Q}H$ denotaremos por $I_q(\alpha)$ o conjunto $I_q(\alpha) = \{g \in H \mid a_g = q\}$.

Tal conjunto é uma ferramenta muito útil para determinar o S-anel $\langle\langle x_1, \ldots, x_k\rangle\rangle$. O próximo resultado é conhecido como *princípio de Schur-Wielandt.*

**Proposição 3.2.3.** *Se $\mathcal{A}$ é um S-anel sobre um grupo $H$ então $\widehat{I}_q(x) \in \mathcal{A}$ para cada $x \in \mathcal{A}$ e $q \in \mathbb{Q}$.*

**Demonstração.** Seja $x \in \mathcal{A}$ e $\mathrm{Bsets}(\mathcal{A}) = \{T_0, \ldots, T_d\}$. Como $\mathcal{A}$ é um S-anel sobre $H$ existem $\alpha_1, \ldots, \alpha_d \in \mathbb{Q}$ tais que $x = \sum_{i=0}^{d} \alpha_i \widehat{T}_i$. Portanto $\widehat{I}_q(x) = \sum_{\{T_j \subset H \mid \alpha_j = q\}} \widehat{T}_j \in \mathcal{A}$ pois se existe $t \in T_j$ tal que seu coeficiente em $x$ é igual a $q$ então todos os elementos de $T_j$ terão coeficiente $q$ em $x$. ■

**Exemplo 3.2.4.** Seja $H = \langle g\rangle$ um grupo cíclico de ordem 8. Considere o seguinte subconjunto $S = \{g, g^7, g^4\}$. Então $\widehat{S} = g + g^4 + g^7$ e $\widehat{S}^2 = 3g^0 + 2g^5 + 2g^3 + g^2 + g^6$. Como $\widehat{S}^2 \in \langle\langle \widehat{S}\rangle\rangle$, pelo princípio de Schur-Wielandt temos que $\widehat{I}_1(\widehat{S}^2) = g^2 + g^6$, $\widehat{I}_2(\widehat{S}^2) = g^5 + g^3, \widehat{I}_3(\widehat{S}^2) = g^0 \in \langle\langle \widehat{S}\rangle\rangle$. Portanto, $g^0, g + g^4 + g^7, g^5 + g^3, g^2 + g^6 \in \langle\langle \widehat{S}\rangle\rangle$.

Agora, $(g^2 + g^6)^2 = 2g^0 + 2g^4$ logo $\frac{1}{2}(g^2 + g^6)^2 - g^0 = g^4 \in \langle\langle \widehat{S}\rangle\rangle$ pois $\langle\langle \widehat{S}\rangle\rangle$ é um S-anel sobre $H$.

Pelo Teorema 3.1.12, $\widehat{S} \circ g^4$ pertence a $\langle\langle \widehat{S}\rangle\rangle$. Além disso, $\widehat{S} - (\widehat{S} \circ g^4) = g + g^7$ o que nos mostra que os elementos $g^0, g + g^7, g^4, g^5 + g^3, g^2 + g^6$ pertencem a $\langle\langle \widehat{S}\rangle\rangle$.

**Afirmação 3.2.5.** *O espaço vetorial $V = \langle g^0, g + g^7, g^4, g^5 + g^3, g^2 + g^6\rangle$ sobre $\mathbb{Q}$, gerado pelos elementos $g^0, g + g^7, g^4, g^5 + g^3, g^2 + g^6$ é um S-anel sobre $H$.*

**Demonstração.** Um cálculo direto nos mostra que $V$ é uma subalgebra de $\mathbb{Q}H$. Para a verificação que $V$ é S-anel sobre $H$ vamos aplicar o Teorema 3.1.12.

Primeiramente, temos que $g^0 \in V$ e como $V$ é um espaço vetorial $g^0 + (g + g^7) + g^4 + (g^5 + g^3) + (g^2 + g^6) = \widehat{H} \in V$.

Dados $\alpha = \alpha_1 g^0 + \alpha_2(g + g^7) + \alpha_3 g^4 + \alpha_4(g^5 + g^3) + \alpha_5(g^2 + g^6)$ e $\beta = \beta_1 g^0 + \beta_2(g + g^7) + \beta_3 g^4 + \beta_4(g^5 + g^3) + \beta_5(g^2 + g^6)$ dois elementos de $V$ tem-se que:

$$\alpha \circ \beta = (\alpha_1 + \beta_1)g^0 + (\alpha_2 + \beta_2)(g + g^7) + (\alpha_3 + \beta_3)g^4 + (\alpha_4 + \beta_4)(g^5 + g^3) + (\alpha_5 + \beta_5)(g^2 + g^6)$$

Logo $\alpha \circ \beta \in V$ para todos $\alpha, \beta \in V$.

Finalmente,

$$\begin{aligned}\alpha^* &= \alpha_1(g^0)^* + \alpha_2(g+g^7)^* + \alpha_3(g^4)^* + \alpha_4(g^5+g^3)^* + \alpha_5(g^2+g^6)^* \\ &= \alpha_1(g^0)^{-1} + \alpha_2(g^{-1}+(g^7)^{-1}) + \alpha_3(g^4)^{-1} + \alpha_4((g^5)^{-1}+(g^3)^{-1}) + \alpha_5((g^2)^{-1}+(g^6)^{-1}) \\ &= \alpha_1 g^0 + \alpha_2(g+g^7) + \alpha_3 g^4 + \alpha_4(g^5+g^3) + \alpha_5(g^2+g^6).\end{aligned}$$

Portanto $\alpha^* \in V$ para todo $\alpha \in V$ o que completa a demonstração da afirmação .

Por fim, $\langle\langle\widehat{S}\rangle\rangle$ é o menor S-anel sobre $H$ que contém o elemento $\widehat{S}$ logo $\langle\langle\widehat{S}\rangle\rangle \subseteq V$. Mas como observado acima, os elementos $g^0, (g+g^7), g^4, (g^5+g^3), (g^2+g^6)$ pertencem a $\langle\langle\widehat{S}\rangle\rangle$ portanto todas as combinações lineares destes elementos também pertencem a $\langle\langle\widehat{S}\rangle\rangle$ logo $V \subseteq \langle\langle\widehat{S}\rangle\rangle$. Consequentemente $\langle\langle\widehat{S}\rangle\rangle = \langle g^0, g+g^7, g^4, g^5+g^3, g^2+g^6\rangle$ ou equivalentemente, $\mathrm{Bsets}(\langle\langle\widehat{S}\rangle\rangle) = \{\{g^0\}, \{g^4\}, \{g, g^7\}, \{g^5, g^3\}, \{g^2, g^6\}\}$.

**Proposição 3.2.6.** *Sejam $\mathcal{A}$ um S-anel sobre um grupo $H$, $\eta = \sum_{g\in H} a_g g \in \mathcal{A}$ e $K = supp(\eta)$. Então $\widehat{K}$ pertence à $\mathcal{A}$. Em outras palavras, o suporte de $\eta$ é um $\mathcal{A}$-subconjunto.*

**Demonstração.** Seja $\mathrm{Bsets}(\mathcal{A}) = \{T_0, \ldots, T_d\}$. Como os conjuntos básicos são disjuntos, tem-se que $K = \bigcup\{T_l \mid \alpha_l \neq 0\}$. ■

**Proposição 3.2.7.** *Seja $\mathcal{A}$ um S-anel sobre um grupo $H$. Se $X \subseteq H$ é um $\mathcal{A}$-subconjunto então $\langle X\rangle$, o subgrupo gerado por $X$, é um $\mathcal{A}$-subgrupo.*

**Demonstração.** Por hipótese, $\widehat{X} \in \mathcal{A}$, isto é, $\sum_{x\in X} x \in \mathcal{A}$. Como $\mathcal{A}$ é um anel, $\tau = (\sum_{x\in X} x) + (\sum_{x\in X} x)^2 + \ldots + (\sum_{x\in X} x)^m$ pertence à $\mathcal{A}$. Seja $\sigma = supp(\tau)$. Pela Proposição 3.2.6, $\widehat{\sigma}$ pertence à $\mathcal{A}$. Tomando $m$ suficientemente grande, $\widehat{\sigma}$ coincide com $\widehat{\langle X\rangle}$. ■

**Proposição 3.2.8.** *Seja $\mathcal{A}$ um S-anel sobre um grupo $H$. Se $E$, $F$ são $\mathcal{A}$-subgrupos então $E \cap F$ e $\langle E \cup F\rangle$ também são $\mathcal{A}$-subgrupos.*

**Demonstração.** Sejam $E$ e $F$ $\mathcal{A}$-subgrupos. Inicialmente, notemos que $E \cap F$ e $\langle E \cup F\rangle$ são subgrupos de $H$. Agora, pela Proposição 3.2.2, existem $T_{i_1}, \ldots, T_{i_m}$ e

$T_{j_1}, \ldots, T_{j_s}$ conjuntos básicos de $\mathcal{A}$ tais que $E = \bigcup_{k=1}^{m} T_{i_k}$ e $F = \bigcup_{l=1}^{s} T_{j_l}$. Escrevendo $A = \{T_{i_1}, \ldots, T_{i_m}\}$ e $B = \{T_{j_1}, \ldots, T_{j_s}\}$, temos $E \cap F = \cup\{A \cap B\}$ e $E \cup F = A \cup B$. Portanto $E \cap F$ e $E \cup F$ são uniões de conjuntos básicos de $\mathcal{A}$ e, aplicando novamente a Proposição 3.2.2, $\widehat{E \cap F}$ e $\widehat{E \cup F}$ pertencem à $\mathcal{A}$. Por fim, a Proposição 3.2.7 nos diz que $\langle \widehat{E \cup F} \rangle \in \mathcal{A}$. ■

**Definição 3.2.9.** *Um S-anel $\mathcal{A}$ sobre um grupo $H$ diz-se* **primitivo** *se não contém $\mathcal{A}$-subgrupos não triviais; equivalentemente, se $K$=1 e $K$=$H$ são os únicos subgrupos de $H$ para os quais vale $\widehat{K} \in \mathcal{A}$. Caso contrário, $\mathcal{A}$ diz-se* **imprimitivo**.

Seja $\mathcal{A}$ um S-anel sobre um grupo $H$. Para cada $T \in \text{Bsets}(\mathcal{A})$ definimos o **estabilizador à esquerda de T** e o **estabilizador à direita de T** como sendo $L(T) = \{h \in H \mid hT = T\}$ e $R(T) = \{h \in H \mid Th = T\}$ respectivamente. Por fim, o **estabilizador de T** é o conjunto $\text{St}(T) = L(T) \cap R(T)$. Estes conjuntos coincidem no caso em que $H$ é abeliano.

**Lema 3.2.10.** *$R(T)$ é um subgrupo de $H$.*

**Demonstração.** Sejam $h_1, h_2$ elementos de $R(T)$. Vamos mostrar que $h_1h_2$ é um elemento de $R(T)$. De fato, temos $T(h_1h_2) = (Th_1)h_2 = Th_2 = T$. O que nos mostra que $h_1h_2 \in R(T)$.

Por fim dado $h \in R(T)$ tem-se $Th = T$ o que implica $T = Th^{-1}$ mostrando que $h^{-1} \in R(T)$. ■

Analogamente, mostra-se que $L(T)$ é um subgrupo de $H$ e portanto $\text{St}(T) = L(T) \cap R(T)$ também o é. A próxima proposição nos mostra a principal propriedade dos conjuntos $L(T), R(T)$ e $\text{St}(T)$ e para demonstrá-la precisamos do seguinte

**Lema 3.2.11.** *Seja $\mathcal{A}$ um S-anel sobre um grupo $H$. Se $T \in$ Bsets$(\mathcal{A})$ então $L(T) = \{h \in T \mid \theta_h(\widehat{T}\widehat{T^{(-1)}}) = |T|\}$.*

**Demonstração.** Inicialmente, notemos que dado $T \in \text{Bsets}(\mathcal{A})$, tem-se que $T^{(-1)} \in \text{Bsets}(\mathcal{A})$ pois $\mathcal{A}$ é um S-anel. Seja $h \in L(T)$ então , pelo Lema 3.1.3, $\theta_h(\widehat{T}\widehat{T^{(-1)}}) = |T \cap h(T^{(-1)})^{(-1)}| = |T \cap hT| = |T|$.

Agora, seja $h \in H$ tal que $\theta_h(\widehat{T}\widehat{T^{(-1)}}) = |T|$. Note que se $t \in T$ existe um único $\tilde{t} \in T$ tal que $h = t\tilde{t}^{-1}$. Como $\theta_h(\widehat{T}\widehat{T^{(-1)}}) = |T|$ e $T \cap hT \subseteq T$ temos que $T \cap hT = T$ o que implica que $T \subseteq hT$. Além disso, suponha por absurdo que existe $t_1$ em $T$ tal que para todo $t$ em $T$ $ht_1 \neq t$. Então $\theta_h(\widehat{T}\widehat{T^{(-1)}}) < |T|$ uma contradição. Portanto $hT = T$, ou seja, $h \in L(T)$. ■

**Proposição 3.2.12.** *Seja $\mathcal{A}$ um S-anel sobre um grupo $H$. Se $T \in \text{Bsets}(\mathcal{A})$ então $L(T), R(T)$ e $\text{St}(T)$ são $\mathcal{A}$-subgrupos e $|R(T)| \leqslant |T|$, $|L(T)| \leqslant |T|$.*

**Demonstração.** Usando a Proposição 3.2.3, os Lemas 3.2.10 e 3.2.11 temos que $\widehat{L(T)} = \widehat{I_q}(\widehat{T}\widehat{T^{(-1)}}) \in \mathcal{A}$ onde $q = |T|$. Analogamente, mostra-se que $\widehat{R(T)} \in \mathcal{A}$. Aplicando a Proposição 3.2.8 concluímos que $\widehat{\text{St}(T)}$ pertence à $\mathcal{A}$. ■

**Proposição 3.2.13.** *Sejam $\mathcal{A}$ um S-anel sobre um grupo $H$, $\eta = \sum_{h \in H} c_h h \in \mathcal{A}$. Dada uma função $f\colon \mathbb{Q} \longrightarrow \mathbb{Q}$ qualquer definimos $f[\eta] = \sum_{h \in H} f(c_h)h$. Então $f[\eta] \in \mathcal{A}$.*

**Demonstração.** Seja $\eta \in \mathcal{A}$, escrevendo $\text{Bsets}(\mathcal{A}) = \{T_0 \ldots, T_d\}$, existem $\alpha_1, \ldots, \alpha_d$ em $\mathbb{Q}$ tais que $\eta = \sum_{k=0}^{d} \alpha_k \widehat{T_k}$. Assim $f[\eta] = \sum_{k=0}^{d} f(\alpha_k)\widehat{T_k}$. Como $f(\alpha_k) \in \mathbb{Q}$ para todo $k, 0 \leqslant k \leqslant d$ então $f[\eta] \in \mathcal{A}$. ■

Vamos introduzir aqui uns conceitos que usaremos na demonstração da próxima Proposição.

**Definição 3.2.14.** *Para cada inteiro $m \in \mathbb{Z}$ e $x = \sum_{h \in H} \alpha_h h \in \mathbb{Q}H$ definimos $x^{(m)} = \sum_{h \in H} \alpha_h h^m$.*

Notemos ainda que vale a seguinte propriedade:

$$\eta^{(mm')} = \left(\eta^{(m)}\right)^{(m')} \text{ para todo } \eta \in \mathbb{Q}H \; m, m' \in \mathbb{Z}. \tag{3.2}$$

**Definição 3.2.15.** *Um elemento* $x = \sum_{h \in H} x_h h$ *em* $\mathbb{Q}H$ *diz-se* **inteiro** *se* $x_h \in \mathbb{Z}$ *para todo* $h \in H$. *Se* $x = \sum_{h \in H} x_h h$ *e* $y = \sum_{h \in H} y_h h$ *são dois elementos inteiros e* $m \in \mathbb{Z}$ *então diremos que* $x \equiv y$ *mod(m) se* $x_h \equiv y_h$ *mod(m) para todo* $h \in H$.

**Lema 3.2.16.** *Sejam* $H$ *um grupo abeliano finito e* $p$ *um número primo tal que* $p$ *não divide a ordem de* $H$. *Para todo subconjunto* $T$ *de* $H$ *tem-se que* $\widehat{T}^{(p)}$ *é uma quantidade simples de* $\mathbb{Q}H$.

**Demonstração.** Seja $T$ um subconjunto qualquer de $H$. Assim $\widehat{T}^{(p)} = \sum_{t \in T} t^p$.

Suponhamos, por absurdo, que existem $t_1$ e $t_2$ distintos em $T$ tais que $t_1^p = t_2^p$. Como $H$ é um grupo abeliano, a igualdade $t_1^p = t_2^p$ implica que $(t_1 t_2^{-1})^p = 1$. Logo a ordem do elemento $t_1 t_2^{-1}$ divide $p$. Como $p$ é um número primo e $t_1 \neq t_2$ então $o(t_1 t_2^{-1}) = p$ o que é uma contradição pois $p$ não divide a ordem de $H$. Consequentemente, $\widehat{T}^{(p)}$ é uma quantidade simples de $\mathbb{Q}H$. ■

**Proposição 3.2.17.** *Seja* $\mathcal{A}$ *um S-anel sobre um grupo abeliano* $H$. *Se* $T \in \text{Bsets}(\mathcal{A})$ *e* $m$ *é um inteiro tal que* $\text{mdc}(m, |H|) = 1$ *então* $T^{(m)} = \{t^m \mid t \in T\}$ *pertence à* $\text{Bsets}(\mathcal{A})$.

**Demonstração.** Primeiramente, seja $p$ um número primo tal que $p \nmid |H|$. Vamos mostrar que se $T \in \text{Bseta}(\mathcal{A})$ então $\widehat{T}^{(p)} \in \mathcal{A}$.

Dado $T = \{t_1, \ldots, t_n\} \in \text{Bsets}(\mathcal{A})$, escrevendo $x = (t_2 + \ldots + t_n)$ e aplicando o Teorema Binomial temos que

$$(t_1 + x)^p = t_1^p + \binom{p}{1} t_1^{p-1} x + \binom{p}{2} t_1^{p-2} x^2 + \ldots + \binom{p}{p-1} t_1 x^{p-1} + x^p;$$

portanto $(t_1 + x)^p \equiv t_1^p + x^p$ *mod(p)*, pois cada parcela $\binom{p}{i} t_1^{p-i} x^i$, $1 \leqslant i \leqslant p-1$, é um

número inteiro múltiplo de $p$. Usando indução sobre $n$ mostra-se que $x \equiv t_2^p + \ldots + t_n^p \; mod(p)$. Portanto podemos concluir que $(\widehat{T})^p \equiv \widehat{T}^{(p)} \; mod(p)$.

Para cada $x \in \mathbb{Z}$ definimos

$$f_p(x) = \text{ o resto da divisão de } x \text{ por } p.$$

Assim $f_p[(\widehat{T})^p] = f_p[\widehat{T}^{(p)}]$. Como $(\widehat{T})^p \in \mathcal{A}$, pela Proposição 3.2.13, $f_p[(\widehat{T})^p] \in \mathcal{A}$ implicando que $f_p[\widehat{T}^{(p)}] \in \mathcal{A}$. Além disso, $p$ não divide $|H|$ logo, pelo Lema 3.2.16, $\widehat{T}^{(p)}$ é uma quantidade simples de $\mathbb{Q}H$ e portanto $f_p[\widehat{T}^{(p)}] = f_p(1)t_1^p + \ldots + f_p(1)t_n^p = \widehat{T}^{(p)} \in \mathcal{A}$.

Considere a função linear $\psi \colon \mathcal{A} \longrightarrow \mathcal{A}$ definida por $\psi(\widehat{T}) = \widehat{T}^{(p)}$, para todo $T \in$ Bsets$(\mathcal{A})$. Dados $T, S$ conjuntos básicos de $\mathcal{A}$ tem-se que

$$\psi(\widehat{T}\widehat{S}) = \sum_{t \in T} \sum_{s \in S} (ts)^p = \sum_{t \in T} \sum_{s \in S} t^p s^p = \left( \sum_{t \in T} t^p \right) \left( \sum_{s \in S} s^p \right) = \widehat{T}^{(p)} \widehat{S}^{(p)} = \psi(\widehat{T})\psi(\widehat{S}).$$

Portanto, $\psi$ é um automorfismo de $\mathcal{A}$ e manda base em base. Consequentemente o conjunto $\{\widehat{T}^{(p)} \mid T \in \text{Bsets}(\mathcal{A})\}$ é uma base de $\mathcal{A}$ formada por quantidades simples de $\mathbb{Q}H$. Além disso, temos que $\widehat{T^{(p)}} = \widehat{T}^{(p)}$ e, usando a Proposição 3.1.5, podemos concluir que $T^{(p)} \in$ Bsets$(\mathcal{A})$.

Finalmente, suponhamos que $m = \prod_{i=1}^{s} p_i$ com $p_i$ números primos tais que $p_i \nmid |H|$ para todo índice $1 \leqslant i \leqslant s$. Como demonstrado acima, $T^{(p_i)} \in$ Bsets$(\mathcal{A})$ e neste caso aplicamos a Propriedade (3.2) e obtemos que $T^{(m)} \in$ Bsets$(\mathcal{A})$. O caso $m = -\prod_{i=1}^{s} p_i$ é análogo. ■

**Proposição 3.2.18.** *Seja $\mathcal{A}$ um S-anel sobre um grupo $H$. Se $T$ e $\{m\}$ pertencem à* Bsets*$(\mathcal{A})$ então $Tm = \{tm \mid t \in T\}$ pertence à* Bsets*$(\mathcal{A})$.*

**Demonstração.** Seja $T = \{t_1, \ldots, t_n\}$. Vamos mostrar que $\widehat{Tm} \in \mathcal{A}$. Temos $\widehat{Tm} = \sum_{t \in T} (tm) = (\sum_{t \in T} t)m = \widehat{T}m = \widehat{T}\widehat{\{m\}} \in \mathcal{A}$ pois $\widehat{T}, \widehat{\{m\}} \in \mathcal{A}$.

Agora, suponhamos que $\widehat{T}\widehat{\{m\}} = \widehat{T_{j_1}} + \widehat{T_{j_2}} + \ldots + \widehat{T_{j_t}}$ onde $T_{j_i} \in$ Bsets$(\mathcal{A})$. Com isso, cada $T_{j_i}$ está contido propriamente em $Tm$. Seja $T_{j_1} = \{t_{j_1}m, t_{j_2}m, \ldots, t_{j_k}m\}$ com $k < n$. Assim existe $t_i m \in Tm$ tal que $t_i m \notin T_{j_1}$, equivalentemente, existe $t_i \in T$ com a propriedade $t_i \neq t_{j_s}$ para todo $s, 1 \leqslant s \leqslant k$.

Agora pela condição *(S3)* de Definição 3.1.4, $\{m^{-1}\}$ pertence à Bsets($\mathcal{A}$) logo $T_{j_1}m^{-1} \subsetneq T$ e $\theta_t(\widehat{T_{j_1}}\widehat{\{m^{-1}\}}) = 1$ para todo $t \in T$, ou seja, $t \in T_{j_1}m^{-1}$ para todo $t \in T$. Em particular, $t_i = (t_{j_s}m)m^{-1} = t_{j_s}$ o que é uma contradição . Portanto $\widehat{Tm} = \widehat{T_{j_i}}$ para algum $i, 1 \leqslant i \leqslant t$, o que nos mostra que $Tm$ pertence à Bsets($\mathcal{A}$). ■

## 3.3 S-subanéis e S-anéis quociente

O objetivo desta seção é definir subanéis e anéis quociente de S-anéis. Note que dado um subgrupo $E$ de um grupo $H$ tem-se que $\mathbb{Q}E$ é uma subalgebra de $\mathbb{Q}H$.

Sejam $\mathcal{A}$ um S-anel imprimitivo sobre um grupo $H$ e $E$ um $\mathcal{A}$-subgrupo próprio não trivial. Definimos $\mathcal{A}_E$ como sendo $\mathcal{A}_E = \mathcal{A} \cap \mathbb{Q}E$. Claramente $\mathcal{A}_E$ é um S-anel sobre $E$ e Bsets($\mathcal{A}_E$) $= \{T \mid T \in \text{Bsets}(\mathcal{A}) \text{ e } T \subset E\}$.

**Definição 3.3.1.** *Nas condições acima, $\mathcal{A}_E$ diz-se um* **S-subanel** *de $\mathcal{A}$. Se $E \lhd H$, definimos o* **S-anel quociente** *$\mathcal{A}/E$ sobre o grupo $H/E$ como o S-anel com base* Bsets$(\mathcal{A}/E) = \{tE \mid t \in T\}$.

## 3.4 O Módulo de transitividade

Neste seção vamos estudar um certo tipo de S-anel muito importante chamado de *Módulo de transitividade.*

**Definição 3.4.1.** *Seja $H$ um grupo finito. Considere um grupo de permutações $G$ sobre $H$ tal que $R_H \subseteq G$ e sejam $T_0 = \{1\}, T_1, \ldots, T_r$ o conjunto completo de órbitas do estabilizador $G_1 = \{g \in G \mid 1^g = 1\}$. O* **módulo de transitividade** $\mathbf{V}(H, G_1)$ *do grupo $G_1$ é o espaço vetorial sobre $\mathbb{Q}$ gerado por $\widehat{T_i}, 0 \leqslant i \leqslant r$, mais explicitamente, $V(H, G_1)$ é o espaço vetorial sobre $\mathbb{Q}$ gerado pelas quantidades simples correspondentes às órbitas $T_0 = \{1\}, T_1, \ldots, T_r$.*

Daqui por diante, nosso objetivo é mostrar que $\mathrm{V}(H, G_1)$ é um S-anel e para isto precisamos de vários resultados. Primeiramente, dado $x = \sum_{h \in H} c_h h \in \mathbb{Q}H$ e $g \in G \subset \mathrm{Sym}(H)$ definimos $x^g = \sum_{h \in H} c_h h^g$.

**Lema 3.4.2.** *Sejam $H$ um grupo finito e $G \subset \mathrm{Sym}(H)$. Para cada $y \in G$, a classe lateral à direita de $y$ determinada por $G_1$ é:*

$$G_1 y = \{g \in G \mid 1^g = 1^y\}.$$

**Demonstração.** Dado $y \in G$, sabemos que a classe lateral à direita de $y$ em $G_1$ é dada por $G_1 y = \{fy \mid f \in G_1\}$. Vamos mostrar que $G_1 y = \{g \in G \mid 1^g = 1^y\}$. De fato, se $g \in G_1 y$ existe $f \in G_1$ tal que $g = fy$. Assim $1^g = 1^{fy} = 1^y$, ou seja, $g \in \{g \in G \mid 1^g = 1^y\}$.

Por outro lado, se $g$ é tal que $1^g = 1^y$ então $1^{gy^{-1}} = 1$ isto nos diz que $gy^{-1} \in G_1$ e $g = (gy^{-1})y \in G_1 y$. Consequentemente, temos a igualdade desejada. ■

Em particular, $G_1 R_{h^y} = \{g \in G \mid 1^g = 1^{R_{h^y}} = h^y\}$ e
$G_1 R_h y = \{g \in G \mid 1^g = 1^{R_h y} = h^y\}$.

**Lema 3.4.3.** *Sejam $H$ um grupo finito e $G \subset \mathrm{Sym}(H)$ com $R_H \subset G$. Dados $h \in H, g \in G$ então $h^g$ é o único elemento $x$ de $H$ tal que (em $\mathbb{Q}G$) $\widehat{G_1} R_x = \widehat{G_1} R_h g$.*

**Demonstração.** Mostraremos inicialmente que $x$ é o único elemento de $H$ que verifica $G_1 R_x = G_1 R_h g$. De fato, sabemos, pelo Lema 3.4.2, que $G_1 R_{h^g} = \{g \in G \mid 1^g = 1^{R_{h^g}} = h^g\}$ e $G_1 R_h g = \{g \in G \mid 1^g = 1^{R_h g} = h^g\}$ logo $G_1 R_{h^g} = G_1 R_h g$.

Agora, suponhamos que existe $x \in H$ satisfazendo $G_1 R_x = G_1 R_h g$, isto é, se $\tilde{g} \in G_1 R_x$ então verifica $1^{\tilde{g}} = 1^{R_x}$ e, pela igualdade, também verifica $1^{\tilde{g}} = 1^{R_h g}$ donde $1^{R_x} = 1^{R_h g}$ o que significa que $x = h^g$. Com isto provamos nossa afirmação .

Finalmente, note que $G_1 R_x = G_1 R_h g$ se e somente se tem-se que $\widehat{G_1} R_x = \widehat{G_1} R_h g$.■

**Lema 3.4.4.** *Sejam $H$ um grupo finito e $G \subseteq \mathrm{Sym}(H)$ com $R_H \subseteq G$. Dados $x \in \mathbb{Q}H$ e $g \in G$ então $x^g$ é o único elemento $y \in \mathbb{Q}H$ tal que $\widehat{G_1}R_y = \widehat{G_1}R_x g$.*

**Demonstração.** Seja $x = \sum_{h\in H} c_h h \in \mathbb{Q}H$. Pelo Lema 3.4.3 sabemos que $\widehat{G_1}R_{x^g} = \widehat{G_1}\sum_{h\in H} c_h R_{h^g} = \sum_{h\in H} c_h \widehat{G_1}R_{h^g} = \sum_{h\in H} c_h \widehat{G_1}R_h g = \widehat{G_1}R_x g$. Mas como as classes laterais $G_1 h$ são distintas tem-se que os elementos $\widehat{G_1}R_h \in \mathbb{Q}G$ são linearmente independentes. De fato, se $\alpha_1\widehat{G_1}R_{h_1} + \alpha_2\widehat{G_1}R_{h_2} + \ldots + \alpha_n\widehat{G_1}R_{h_n} = 0$ então $1^{[\alpha_1\widehat{G_1}R_{h_1}+\ldots+\alpha_n\widehat{G_1}R_{h_n}]} = 0$, ou seja, $1^{\alpha_1\widehat{G_1}R_{h_1}} + 1^{\alpha_2\widehat{G_1}R_{h_2}} + \ldots + 1^{\alpha_n\widehat{G_1}R_{h_n}} = 0$. Por outro lado, $1^{\alpha_1\widehat{G_1}R_{h_1}} + \ldots + 1^{\alpha_n\widehat{G_1}R_{h_n}} = (\alpha_1|G_1|1)^{R_{h_1}} + \ldots + (\alpha_n|G_1|1)^{R_{h_n}} = \alpha_1|G_1|h_1 + \ldots + \alpha_n|G_1|h_n = 0$. Portanto $\sum_{i=1}^{n} \alpha_i h_i = 0$ implicando que $\alpha_i = 0$ para todo $i, 1 \leqslant i \leqslant n$. Agora, seja $y = \sum_{h\in H} d_h h^g \in \mathbb{Q}H$ tal que $\widehat{G_1}R_y = \widehat{G_1}R_x g$. Então: $\widehat{G_1}R_y = \widehat{G_1}\sum_{h\in H} d_h R_{h^g} = \sum_{h\in H} d_h \widehat{G_1}R_{h^g} = \sum_{h\in H} c_h \widehat{G_1}R_h g = \sum_{h\in H} c_h \widehat{G_1}R_{h^g} = \widehat{G_1}R_{x^g}$. Como os elementos da forma $G_1R_h, h \in H$, são linearmente independentes temos que $d_h = c_h$ para todo $h \in H$ mostrando que $y = x^g$. ■

**Lema 3.4.5.** *Sejam $H$ um grupo finito e $G \subseteq \mathrm{Sym}(H)$ com $R_H \subseteq G$. Dado $x \in \mathbb{Q}H$ então $x \in V(H, G_1)$ se e somente se $x^g = x$ para todo $g \in G_1$.*

**Demonstração.** Seja $x = \sum_{h\in H} c_h h \in \mathbb{Q}H$. Suponhamos que $x \in V(H, G_1)$. Existem $\alpha_1, \ldots, \alpha_r \in \mathbb{Q}$ tais que $x = \sum_{i=0}^{r} \alpha_k \widehat{T_k}$. Logo $x^g = \sum_{i=0}^{r} \alpha_k (\widehat{T_k})^g = \sum_{i=0}^{r} \alpha_k \widehat{T_k^g}$ para todo $g \in G_1$. Observe que para todo $t \in T_k$ existem $h \in H$ e $g_1 \in G_1$ tais que $t = h^{g_1}$ uma vez que cada $T_k$ é uma órbita do grupo $G_1$. Portanto $t^g = (h^{g_1})^g = h^{g_1 g} \in T_k$.

Mostramos que se $t \in T_k$ então $t^g \in T_k$ para todo $g \in G_1$. Consequentemente $x^g = \sum_{i=0}^{r} \alpha_k (\widehat{T_k})^g = \sum_{i=0}^{r} \alpha_k \widehat{T_k^g} = \sum_{i=0}^{r} \alpha_k \widehat{T_k} = x$.

Reciprocamente, suponhamos que $x^g = x$ para todo $g \in G_1$. Assim $x^g = \sum_{h\in H} c_h h^g = \sum_{h\in H} c_h h = x$. Logo $c_{h^g} = c_h$ para todo $g \in G_1$, ou seja, os elementos que estão na mesma órbita têm o mesmo coeficiente em $x$; portanto $x \in V(H, G_1)$. ■

**Lema 3.4.6.** *Sejam $H$ um grupo finito e $G \subseteq \mathrm{Sym}(H)$ com $R_H \subseteq G$. Dado $x \in \mathbb{Q}H$, são equivalentes.*

1. $x \in V(H, G_1)$
2. *se* $u \in G_1$ *então* $\widehat{G_1} R_x u = \widehat{G_1} R_x$
3. $\widehat{G_1} R_x \widehat{G_1} = |G_1| \widehat{G_1} R_x$

**Demonstração.** (1) $\Leftrightarrow$ (2). Seja $x \in \mathbb{Q}H$. Aplicando os Lemas 3.4.4 e 3.4.5, temos

$$x \in V(H, G_1) \Leftrightarrow x^u = x \Leftrightarrow \widehat{G_1} R_{x^u} = \widehat{G_1} R_x = \widehat{G_1} R_x u.$$

(2) $\Rightarrow$ (3). Temos:

$$\begin{aligned}\widehat{G_1} R_x \widehat{G_1} &= \sum_{u \in G_1} \widehat{G_1} R_x u \\ &= \sum_{u \in G_1} \widehat{G_1} R_x \\ &= |G_1| \widehat{G_1} R_x.\end{aligned}$$

(3) $\Rightarrow$ (2) Se $u \in G_1$ então

$|G_1| \widehat{G_1} R_x u = \widehat{G_1} R_x \widehat{G_1} u = \widehat{G_1} R_x \widehat{G_1} = |G_1| \widehat{G_1} R_x$. Logo $\widehat{G_1} R_x u = \widehat{G_1} R_x$. ■

**Lema 3.4.7.** *Sejam $H$ um grupo finito e $G \subseteq \mathrm{Sym}(H)$ com $R_H \subseteq G$. Dado $x \in \mathbb{Q}H$ tem-se que $x \in V(H, G_1)$ se e somente se $\widehat{G_1} R_x = R_x \widehat{G_1}$.*

**Demonstração.** ($\Rightarrow$) Suponhamos que $x \in V(H, G_1)$. Como $V(H, G_1)$ é gerado como espaço vetorial sobre $\mathbb{Q}$ pelas quantidades simples correspondentes às órbitas $T_0 = \{1\}, T_1, \ldots, T_r$ do grupo $G_1$ é suficiente provarmos o resultado para $x = \widehat{T}$ onde $T$ é uma órbita de $G_1$. Pelo Lema 3.4.6, $\widehat{G_1} R_{\widehat{T}} \widehat{G_1} = |G_1| \widehat{G_1} R_{\widehat{T}}$. Com isso e com o fato que $R_{\widehat{T}} = \widehat{R_T}$ temos $G_1 R_T G_1 = G_1 R_T$ e $R_T G_1 \subset G_1 R_T$. Como $T$ é um subconjunto de $H$ e $R_H \cap G_1 = 1$ então $|R_T G_1| = |R_T||G_1| = |G_1 R_T|$ logo $R_T G_1 = G_1 R_T$. De fato, se existir $t_1, t_2 \in T$ e $g_1, g_2 \in G_1$ distintos tais que $R_{t_1} g_1 = R_{t_2} g_2$ teremos $R_{t_1^{-1} t_2} = g_1 g_2^{-1} \in R_H \cap G_1 = 1$ implicando que $t_1 = t_2$ o que é uma contradição pois tomamos $t_1, t_2$ distintos. Por fim, $\widehat{G_1} R_x = \widehat{G_1} R_{\widehat{T}} = R_{\widehat{T}} \widehat{G_1} = R_x \widehat{G_1}$.

($\Leftarrow$) Suponhamos que $\widehat{G_1}R_x = R_x\widehat{G_1}$. Assim $\widehat{G_1}R_x\widehat{G_1} = \widehat{G_1}^2R_x = |G_1|\widehat{G_1}R_x$ portanto, pelo Lema 3.4.6, $x \in V(H, G_1)$. ■

**Lema 3.4.8.** *Sejam $H$ um grupo finito, $G \subseteq \mathrm{Sym}(H)$ com $R_H \subseteq G$, $x \in V(H, G_1), g \in G$ e $\eta \in \mathbb{Q}H$. Então $(x\eta)^g = x\eta^g$.*

**Demonstração.** Pelos Lemas 3.4.4 e 3.4.7 temos:
$\widehat{G_1}R_xR_{(\eta^g)} = R_x\widehat{G_1}R_{(\eta^g)} = R_x\widehat{G_1}R_\eta g = \widehat{G_1}R_xR_\eta g = \widehat{G_1}R_{x\eta}g = \widehat{G_1}R_{(x\eta)^g}g$. Como $x\eta^g \in \mathbb{Q}H$, pelo Lema 3.4.4 novamente, $x\eta^g = (x\eta)^g$. ■

Diante destes fatos, temos o seguinte

**Teorema 3.4.9.** *Sejam $H$ um grupo finito e $G \subseteq \mathrm{Sym}(H)$ com $R_H \subseteq G$. Então o módulo de transitividade do grupo $G_1$, $V(H, G_1)$, é um S-anel sobre $H$.*

**Demonstração.** Seja $H$ um grupo finito. Considere um grupo de permutações $G$ sobre $H$ tal que $R_H \subseteq G$. Denote por $T_0 = \{1\}, T_1, \ldots, T_r$ o conjunto completo de órbitas do estabilizador $G_1 = \{g \in G \mid 1^g = 1\}$.

Por definição , $V(H, G_1)$ é um subespaço vetorial de $\mathbb{Q}H$. Precisamos mostrar que é fechado pela multiplicação. De fato, dados $x$ e $y$ dois elementos quaisquer de $V(H, G_1)$ e dado $u \in G_1$, pelos Lemas 3.4.5 e 3.4.8 temos $(xy)^u = xy^u = xy$ o que nos mostra que $xy \in V(H, G_1)$. Assim $V(H, G_1)$ é uma subalgebra de $\mathbb{Q}H$.

Além disto, verifica-se facilmente que $V(H, G_1)$ satisfaz as condições (S1) e (S2) da Definição 3.1.4.

Por fim, sejam $x, y \in T_i$ e $x^{-1} \in T_j$. Existe $g \in G_1$ tal que $x^g = y$. Logo $1^{R_xgR_{y^{-1}}} = x^{gR_{y^{-1}}} = y^{R_{y^{-1}}} = 1$, ou seja, $R_xgR_{y^{-1}} \in G_1$ e $(x^{-1})^{R_xgR_{y^{-1}}} = 1^{gR_{y^{-1}}} = 1^{R_{y^{-1}}} = y^{-1}$. Em outras palavras, $y^{-1} \in T_j$ mostrando que para todo índice $i, 0 \leqslant i \leqslant d$, existe um índice $j, 0 \leqslant j \leqslant d$, tal que $T_j = T_i^{(-1)}$. ■

A implicação contrária não é verdadeira, isto é, nem todo S-anel é o módulo de transitividade de um grupo apropriado. Veja [13], Teorema 26.4. Isto nos motiva a introduzir a seguinte

**Definição 3.4.10.** *Seja $H$ um grupo finito. Um S-anel $\mathcal{A}$ sobre $H$ diz-se* **Schuriano** *se existe $G \subseteq \mathrm{Sym}(H)$ com $R_H \subseteq G$ tal que $\mathcal{A} = V(H, G_1)$. Em outras palavras, $\mathcal{A}$ diz-se* **Schuriano** *se $\mathcal{A}$ é o módulo de transitividade do grupo $G_1$ de algum $G \subseteq \mathrm{Sym}(H)$ com $R_H \subseteq G$.*

Para terminar este capítulo, vamos dar uma aplicação do Teorema 3.4.9.

**Teorema 3.4.11.** *Sejam $H$ um grupo finito e $G \subseteq \mathrm{Sym}(H)$ com $R_H \subseteq G$. Então $G$ é um grupo de permutações primitivo se e somente se o módulo de transitividade do grupo $G_1$ é um S-anel primitivo.*

**Demonstração.** ($\Rightarrow$) Se $V(H, G_1)$ é um S-anel imprimitivo existe um subgrupo $K$ de $H$ tal que $1 < K < H$ e $\widehat{K} \in V(H, G_1)$. Pelo Lema 3.4.7, $R_{\widehat{K}}\widehat{G_1} = \widehat{G_1}R_{\widehat{K}}$. Mas $R_{\widehat{K}} = \widehat{R_K}$ logo $G_1R_K = Z$ é um subgrupo de $G$ de ordem $|G_1||R_K|$ assim $G_1 < Z < G$ e, pelo Corolário 1.1.2, $G$ é imprimitivo.

($\Leftarrow$) Se $G$ não é primitivo então existe um subgrupo $L$ de $G$ tal que $G_1 < L < G$. Mas $G = G_1R_H$, de fato, dado $g \in G$ podemos reescrevê-lo da seguinte maneira $g = (gR_h)R_{h^{-1}}$ onde $h = (1^g)^{-1}$. Com isso, $L = G_1K$ para algum subgrupo $K$ de $R_H$. Note que $1 < K < R_H$ e $\widehat{G_1}\widehat{K} = \widehat{L} = \widehat{L}^* = \widehat{K}^*\widehat{G_1}^* = \widehat{K}\widehat{G_1}$ e, pelo Lema 3.4.7, $\widehat{K} \in V(H, G_1)$ portanto $V(H, G_1)$ é um S-anel imprimitivo. ■

# Capítulo 4

# p-S-anéis

Neste capítulo vamos estudar um tipo especial de anéis de Schur. Em particular, vamos classificar tais S-anéis sobre o grupo $\mathbb{Z}_p^3$.

## 4.1 p-S-anéis sobre $Z_p^3$

**Definição 4.1.1.** *Seja $p$ um número primo. Um* **p-S-anel** *é um S-anel sobre um p-grupo $H$ e tal que a cardinalidade de todo conjunto básico é uma potência de $p$.*

**Proposição 4.1.2.** *Seja $\mathcal{A}$ um p-S-anel sobre um p-grupo $H$. Então o conjunto*

$$\mathcal{O}_*(\mathcal{A}) = \{h \in H \mid \{h\} \in \mathrm{Bsets}(\mathcal{A})\}$$

*é um $\mathcal{A}$-subgrupo não trivial de $H$.*

**Demonstração.** Seja $\mathrm{Bsets}(\mathcal{A}) = \{T_0, \ldots, T_d\}$.

Vamos inicialmente mostrar que $\mathcal{O}_*(\mathcal{A})$ é um subgrupo de $H$. Sejam $h_1, h_2$ elementos de $H$ tais que $\{h_1\}, \{h_2\} \in \mathrm{Bsets}(\mathcal{A})$. Assim $\widehat{\{h_1\}} = h_1$ e $\widehat{\{h_2\}} = h_2$ logo $\widehat{\{h_1\}}\widehat{\{h_2\}} = h_1h_2 = \sum_{k=0}^{d} \alpha_k \widehat{T_k}$. Então existe um índice $j, 0 \leqslant j \leqslant d$, satisfazendo $T_j = \{h_1h_2\}$. Portanto $\{h_1h_2\} \in \mathrm{Bsets}(\mathcal{A})$, ou seja, $h_1h_2 \in \mathcal{O}_*(\mathcal{A})$.

Agora, se $h \in \mathcal{O}_*(\mathcal{A})$ pela condição *(iii)* de Definição 3.1.4, $h^{-1} \in \mathcal{O}_*(\mathcal{A})$ mostrando que $\mathcal{O}_*(\mathcal{A})$ é um subgrupo de $H$. Além disso, podemos escrever $\mathcal{O}_*(\mathcal{A}) = \bigcup\{h\}$ onde

$h \in \mathcal{O}_*(\mathcal{A})$, isto é, $\mathcal{O}_*(\mathcal{A})$ é uma união de conjuntos básicos de $\mathcal{A}$ portanto é um $\mathcal{A}$-subgrupo de $H$.

Por fim, veremos que $\mathcal{O}_*(\mathcal{A})$ não é trivial. Se $\mathcal{O}_*(\mathcal{A}) = \{1\}$ então para todo $T_i$ em Bsets($\mathcal{A}$) com $T_i \neq \{1\}$ temos $|T_i| = p^{n_i}$ onde $n_i \in \mathbb{N}, n_i \neq 0$. Mas sabemos que $|H| = p^m$ logo $p^m = 1 + p^{n_1} + \ldots + p^{n_d} \Rightarrow p^m - p\alpha = 1 \Rightarrow p(p^{m-1} - \alpha) = 1 \Rightarrow p \mid 1$ o que é uma contradição pois $p > 1$. Portanto $\mathcal{O}_*(\mathcal{A}) \neq \{1\}$. ■

Seja $\mathcal{A}$ um $p$-S-anel sobre um grupo $H$. Dado um conjunto básico $T$ de $\mathcal{A}$, consideremos o seguinte conjunto:

$$T^{-1}T = \{x^{-1}y \mid x, y \in T\}.$$

Também vale a seguinte

**Proposição 4.1.3.** *Nas condições acima, o conjunto*

$$\mathcal{O}^*(\mathcal{A}) = \langle\{\bigcup T^{-1}T \mid T \in \text{Bsets}(\mathcal{A})\}\rangle$$

*é um $\mathcal{A}$-subgrupo próprio de $H$.*

Este resultado segue de fatos mais gerais sobre configurações coerentes e sobre esquemas de associação (veja [14], também citado em [6]). Não incluiremos aqui a demonstração porque envolve muitos pré-requisitos e nos levaria longe demais dos resultados que interessam nesta dissertação .

**Lema 4.1.4.** *Seja $H$ um $p$-grupo abeliano elementar de posto dois e $\mathcal{B}$ um $p$-S anel sobre $H$. Então ou* Bsets($\mathcal{B}$) $= \{\{h\} \mid h \in H\}$ *(o que é equivalente a dizer que $\mathcal{B} = \mathbb{Q}H$) ou existem um subgrupo $L$ de $H$ de ordem $p$ e um elemento $y \in H \setminus L$ tais que* Bsets($\mathcal{B}$) $= \{Ly^i \mid 1 \leqslant i \leqslant p-1\} \cup \{\{l\} \mid l \in L\}$.

**Demonstração.** Note que $|H| = p^2$ donde $|T| = 1$ ou $p$ para todo conjunto básico de $\mathcal{B}$.

Suponhamos que existe $T$ em Bsets($\mathcal{B}$) com $|T| = p$. Pela Proposição 4.1.3, temos $p = |T| \leqslant |TT^{-1}| \leqslant |\mathcal{O}^*(\mathcal{B})| \leqslant p$ e como $TT^{-1} \subseteq \mathcal{O}^*(\mathcal{B})$ temos que $TT^{-1} = \mathcal{O}^*(\mathcal{B})$.

Assim, dado qualquer elemento $t$ em $T$ temos que $Tt^{-1} \subseteq \mathcal{O}^*(\mathcal{B})$ com $|Tt^{-1}| = p = |\mathcal{O}^*(\mathcal{B})|$. Isto nos diz que $T = \mathcal{O}^*(\mathcal{B})t$.

Denotando $\mathcal{O}^*(\mathcal{B})$ por $L$ para simplificar a notação, a Proposição 3.2.17 nos diz que $Lt, Lt^2, \ldots, Lt^{p-1}$ são elementos do conjunto Bsets($\mathcal{B}$).

**Afirmação 4.1.5.** *$Lt, Lt^2, \ldots, Lt^{p-1}$ são conjuntos distintos.*

De fato, se existem inteiros $1 \leqslant a, b \leqslant p-1$ tais que $Lt^a = Lt^b$ então $t^{(a-b)} \in L$. Com isso, a classe $Lt$ tem ordem $(a-b)$ no grupo $H/L$. Mas a ordem do grupo $H/L$ é igual a $p$ logo $(a-b)$ divide $p$ o que não pode acontecer pois $1 \leqslant a, b \leqslant p-1$.

Por outro lado, como $L$ é um $\mathcal{B}$-subgrupo de ordem $p$ e $1 \in L$ não existe nenhum conjunto básico de $\mathcal{B}$ com cardinalidade $p$ contido em $L$ senão teríamos $|L| > p$ portanto todos os conjuntos unitários $\{l\}$ com $l \in L$ são conjuntos básicos de $\mathcal{B}$.

Assim tem-se que ou $|T| = 1$ para todo conjunto básico $T$ de $\mathcal{B}$ e, neste caso Bsets($\mathcal{B}$) $= \{\{h\} \mid h \in H\}$, ou existe um conjunto básico $T$ de $\mathcal{B}$ com $|T| = p$ e, neste caso, existem um subgrupo $L$ de $H$ de ordem $p$ e um elemento $y \in H \setminus L$ tais que Bsets($\mathcal{B}$) $= \{Ly^i \mid 1 \leqslant i \leqslant p-1\} \cup \{\{l\} \mid l \in L\}$. ■

Em [6], os autores, Muzychuk e Hirasaka, interessados em determinar a estrutura dos $p$-$S$-anéis sobre um grupo $H$ abeliano elementar de posto 3, mostraram que existe um único (a menos de isomorfismo) $p$-$S$-anel Schuriano $\mathcal{A}$ sobre $H$ tal que Bsets($\mathcal{A}$) contém um conjunto básico de cardinalidade $p$ e $\langle T \rangle = H$. No entanto não estavam certos da existência de $p$-$S$-anéis não Schurianos sobre $H$ satisfazendo a propriedade citada acima.

P. Spiga e Q. Wang responderam esta questão em [12] com o seguinte

**Teorema 4.1.6** (P.Spiga, Q.Wang). *Seja $H$ um $p$-grupo abeliano elementar de posto 3. Então todo $p$-$S$-anel sobre $H$ é Schuriano.*

Nosso principal objetivo agora é demonstrar este teorema. Para tanto, no que segue $H$ é um $p$-grupo abeliano elementar de posto 3 e $\mathcal{A}$ é um $p$-S-anel sobre $H$.

**Lema 4.1.7.** *Se existe $T$ em* Bsets($\mathcal{A}$) *com* $|T| = p^2$ *então $\mathcal{A}$ é Schuriano.*

**Demonstração.** Seja $T$ em Bsets($\mathcal{A}$) com $|T| = p^2$. Denote por $R$ o subgrupo $\mathcal{O}^*(\mathcal{A})$. Pela Proposição 4.1.3, $p^2 = |T| \leqslant |TT^{-1}| \leqslant |R| \leqslant p^2$. Com isso $TT^{-1} = R$. Isto nos diz que $T$ é uma classe lateral $Rt$ de $R$. Agora, pela Proposição 3.2.17, $Rt, \ldots, Rt^{p-1}$ são $p-1$ elementos de Bsets($\mathcal{A}$).

Provaremos inicialmente que

*Afirmação :* $Rt, \ldots, Rt^{p-1}$ são $p-1$ elementos de Bsets($\mathcal{A}$) distintos. Se existem $1 \leq a, b \leq p-1$ tais que $Rt^a = Rt^b$ então $t^{(a-b)} \in R$. Com isso, a classe $Rt$ tem ordem $(a-b)$ no grupo $H/R$. Mas a ordem do grupo $H/R$ é igual a $p$ logo $(a-b)$ divide $p$, uma contradição , pois $1 \leqslant a, b \leqslant p-1$. Por fim $H \setminus R = \bigcup_{i=1}^{p-1} Rt^i$.

Agora, como $|R| = p^2$, segue que $R$ é um $p$-grupo abeliano elementar de posto 2. Com isso o conjunto $\{U \in \text{Bsets}(\mathcal{A}) \mid U \subseteq R\}$ determina um $p$-S-anel $\mathcal{A}_R$ sobre $R$ e, pelo Lema 4.1.4, temos que ou Bsets($\mathcal{A}_R$) $= \{\{r\} \mid r \in R\}$ ou existem um subgrupo $L$ de $R$ de ordem $p$ e $y \in R \setminus L$ tais que Bsets($\mathcal{A}_R$) $= \{Ly^i \mid 1 \leqslant i \leqslant p-1\} \cup \{\{l\} \mid l \in L\}$.

Portanto podemos concluir que ou

$$\text{Bsets}(\mathcal{A}) = \{\{r\} \mid r \in R\} \cup \{Rt^i \mid 1 \leqslant i \leqslant p-1\}$$

ou existem um subgrupo $L$ de $R$ de ordem $p$ e um elemento $y \in R \setminus L$ tais que

$$\text{Bsets}(\mathcal{A}) = \{Ly^i \mid 1 \leqslant i \leqslant p-1\} \cup \{\{l\} \mid l \in L\} \cup \{Rt^i \mid 1 \leqslant i \leqslant p-1\}.$$

- **Caso 1:** Bsets($\mathcal{A}$) $= \{\{r\} \mid r \in R\} \cup \{Rt^i \mid 1 \leqslant i \leqslant p-1\}$

  Devemos mostrar que existe um grupo $G \in \text{Sup}(R_H)$ tal que o conjunto das órbitas do grupo $G_1$ é exatamente Bsets($\mathcal{A}$).

  Considere o grupo de permutações $G = R_H \rtimes (C_{\text{GL}(H)}(R) \cap C_{\text{GL}(H)}(H/R))$ onde $C_{\text{GL}(H)}(R)$ denota o conjunto dos isomorfismos lineares de $H$ que fixam ponto a ponto $R$ e $C_{\text{GL}(H)}(H/R)$ denota o conjunto dos isomorfismos lineares que fixam as classes laterais de $R$ em $H$. Note que são todas transformações afins.

*Afirmação :* O conjuntos das órbitas do grupo

$$G_1 = (C_{\mathrm{GL}(H)}(R) \cap C_{\mathrm{GL}(H)}(H/R))$$

é exatamente Bsets($\mathcal{A}$).

Seja $T$ um conjunto básico de $\mathcal{A}$. Se $T = \{r\}$ para algum $r \in R$ então $T$ é exatamente a $G_1$-órbita de $r$ pois $r^\varphi = r$ para toda $\varphi \in G_1$.

Por outro lado, suponhamos que $T = Rt^i$ para algum $i$. Dado $rt^i \in T$ vamos mostrar que $T$ é exatamente a $G_1$-órbita de $rt^i$. De fato, para toda $\varphi \in G_1$ tem-se que $(rt^i)^\varphi = r^\varphi (t^i)^\varphi = rr_1t^i \in T$.

Finalmente, dado $\bar{r}t^i$ um elemento qualquer de $T$ definimos a função $f\colon H \longrightarrow H$ que leva $(t^i)$ em $r^{-1}\bar{r}t^i$ e fixa todos os outros elementos. Claramente $f \in G_1$ e $(rt^i)^f = \bar{r}t^i$.

Portanto concluímos que $T$ é exatamente a $G_1$-órbita de $rt^i$ [1].

- **Caso 2:** Bsets($\mathcal{A}$) $= \{Ly^i \mid 1 \leqslant i \leqslant p-1\} \cup \{\{l\} \mid l \in L\} \cup \{Rt^i \mid 1 \leqslant i \leqslant p-1\}$. Devemos mostrar que existe um grupo $G \in \mathrm{Sup}(R_H)$ tal que o conjunto das órbitas do grupo $G_1$ é exatamente Bsets($\mathcal{A}$).

  Considere o grupo de permutações afim

  $$G = R_H \rtimes (C_{\mathrm{GL}(H)}(L) \cap C_{\mathrm{GL}(H)}(R/L) \cap C_{\mathrm{GL}(H)}(H/R))$$

  onde $C_{\mathrm{GL}(H)}(L)$ denota o conjunto dos isomorfismos lineares de $H$ que fixam ponto a ponto $L$, $C_{\mathrm{GL}(H)}(H/R)$ denota o conjunto dos isomorfismos lineares que fixam as classes laterais de $L$ em $R$ e $C_{\mathrm{GL}(H)}(H/R)$ denota o conjunto dos isomorfismos lineares que fixam as classes laterais de $R$ em $H$.

  Procedendo de forma análoga ao Caso 1, obtemos o resultado do Caso 2.

[1] Esta demonstração estava errada no artigo [12]. Nós detectamos o erro e fizemos a correção correspondente e a comunicamos ao autor que concordou com a nossa correção .

Isto nos mostra que $\mathcal{A}$ é um $p$-S-anel Schuriano. ■

Note que se $\mathcal{O}_*(\mathcal{A}) = H$ então $\mathcal{A}$ é Schuriano, mais explicitamente, $\mathcal{A} = V(H, 1_{\mathrm{Sym}(H)})$. Assim vamos assumir que $|T| \leqslant p$ para todo $T$ em $\mathrm{Bsets}(\mathcal{A})$ e $\mathcal{O}_*(\mathcal{A}) \neq H$. Denotaremos por $K$ o subgrupo $\mathcal{O}_*(\mathcal{A})$. Antes do nosso próximo resultado precisamos da seguinte

**Definição 4.1.8.** *Sejam $G$ um grupo abeliano e $L$ um subgrupo de $G$. Um* **transversal** *de $L$ em $G$ é um subconjunto de $G$ formado por exatamente um elemento de cada classe lateral de $L$ em $G$.*

**Lema 4.1.9.** *Se $|K| = p^2$ então $\mathcal{A}$ é Schuriano.*

**Demonstração.** Note, inicialmente, que existe $T$ em $\mathrm{Bsets}(\mathcal{A})$ com $|T| = p$ pois estamos assumindo que $K \neq H$. Como $|\mathrm{St}(T)| \leqslant |T| \leqslant p$ pode ocorrer que $\mathrm{St}(T) = 1$ ou $|\mathrm{St}(T)| = p$.

Se $\mathrm{St}(T) = 1$, pela Proposição 3.2.18, $\{Tx \mid x \in K\}$ pertence a $\mathrm{Bsets}(\mathcal{A})$, ou seja, existem $p^2$ subconjuntos disjuntos de $H$ tal que $\bigcup_{x\in K} Tx \subseteq H$. Por outro lado, $|\bigcup_{x\in K} Tx| = \sum_{x\in K} |Tx| = \underbrace{p + \ldots + p}_{p^2\text{vezes}} = p^3 = |H|$. Portanto $\bigcup_{x\in K} Tx = H$, uma contradição pois se $1 \in Tx$ então $T \cap K \neq \emptyset$ mas $T \cap K = \emptyset$. Concluímos que $\mathrm{St}(T) = L$ é um subgrupo de $K$ de ordem $p$ uma vez que $1 \in \mathrm{St}(T)$. Além disso, dado $t \in T$, temos que $Lt \subseteq T$ com $|Lt| = p = |T|$ logo existe $t \in H \setminus K$ tal que $T = Lt$.

Seja $\{x_1, \ldots, x_p\}$ um transversal de $L$ em $K$. Pelas Proposições 3.2.17 e 3.2.18. temos que $Lt^j x_i \in \mathrm{Bsets}(\mathcal{A})$, para $i = 1, \ldots, p$ e $j = 1, \ldots, p-1$. Isto implica que $\mathrm{Bsets}(\mathcal{A}) = \{Lt^j x_i \mid i = 1, \ldots, p, j = 1, \ldots, p-1\} \cup \{\{k\} \mid k \in K\}$.

Seja $l$ um gerador de $L$ e $\varphi \in \mathrm{GL}(H)$ um isomorfismo que leva $t$ em $tl$ e que fixa todo elemento de $K$. Considere o grupo de permutações $G = R_H \rtimes \langle\varphi\rangle$. Note que $G_1 = \langle\varphi\rangle$.

*Afirmação :* O conjunto das órbitas do grupo $\langle\varphi\rangle$ é exatamente Bsets($\mathcal{A}$).

Seja $T$ um elemento de Bsets($\mathcal{A}$). Se $T = \{k\}$ para algum $k \in K$ então a $\langle\varphi\rangle$-órbita de $k$ é exatamente $T$. Agora, se $T = Lt^jx_i$ para algum $j, 1 \leqslant j \leqslant p-1$ e para algum $i, 1 \leqslant i \leqslant p$, dado $\alpha$ em $T$, existe $l_1 = l^s \in L$ tal que $\alpha = l_1t^jx_i$. Assim $\alpha^\varphi = (l_1t^jx_i)^\varphi = l_1^\varphi(t^j)^\varphi x_i^\varphi = l_1(tl)^jx_i = l_2t^jx_i \in T$. Logo $\alpha^{\varphi^m} \in T$ para todo $1 \leqslant m \leqslant o(\varphi)$. Com isso mostramos que a $\langle\varphi\rangle$-órbita de $\alpha$ está contida em $T$. Por outro lado, se $x$ pertence a $T$, existe $l_2 = l^r$ em $L$ tal que $x = l_2t^jx_i$. Tomando $m = (r-s)/j$ temos $\alpha^{\varphi^m} = l^s(l^{[(r-s)/j]j})t^jx_i = l^rt^jx_i = x$. Concluímos que todo elemento de $T$ é a imagem de $\alpha$ por uma potência da função $\varphi$, ou seja, $T$ é a $\langle\varphi\rangle$-órbita de $\alpha$. Analogamente mostramos que toda órbita do grupo $\langle\varphi\rangle$ é um conjunto básico de $\mathcal{A}$. Portanto $\mathcal{A} = V(H, \langle\varphi\rangle)$. ■

Com este resultado, podemos assumir que o grupo $K$ tem ordem $p$.

**Lema 4.1.10.** *Se* $|\mathrm{St}(T)| = p$ *para todo* $T$ *em* Bsets($\mathcal{A}$) *com cardinalidade* $p$ *então* $\mathcal{A}$ *é Schuriano.*

**Demonstração.** Seja $T$ um conjunto básico de $\mathcal{A}$ com $|T| = p$. A Proposição 3.2.12 nos diz que $\mathrm{St}(T)$ é um $\mathcal{A}$-subgrupo de $H$ e, além disso, $\mathrm{St}(T) \subseteq K$. Por outro lado, $|\mathrm{St}(T)| = p = |K|$ logo $\mathrm{St}(T) = K$. Agora, se existe $x \in T \cap K$ então $\{x\} \in \mathrm{Bsets}(\mathcal{A})$ com $T \cap \{x\} \neq \emptyset$ o que não pode acontecer. Assim $T \cap K = \emptyset$.

Por fim, seja $x \in T$. Sabemos que $x \notin K$ e $K = \mathrm{St}(T)$; logo, para todo $k$ em $K$ temos que $kx \in T$, ou seja, $Kx \subseteq T$. Mas $|Kx| = p = |T|$ implicando que $T = Kx$. Diante deste fato, podemos concluir que todo conjunto básico de $\mathcal{A}$ com cardinalidade $p$ é uma classe lateral de $K$. Assim $\mathrm{Bsets}(\mathcal{A}) = \{\{k\} \mid k \in K\} \cup \{Kx \mid x \in H \setminus K\}$

Seja $\{x, y, k\}$ uma base de $H$ sobre $\mathbb{F}_p$ tal que $k \in K$ e $\varphi_1, \varphi_2$ em $\mathrm{GL}(H)$ tais que:

$$\varphi_1 : \begin{array}{l} x \longmapsto xk \\ y \longmapsto y \\ k \longmapsto k \end{array} \qquad \varphi_2 : \begin{array}{l} x \longmapsto x \\ y \longmapsto yk \\ k \longmapsto k \end{array}$$

Considere o grupo de permutações $G = R_H \rtimes \langle\varphi_1, \varphi_2\rangle$. Assim $G_1 = \langle\varphi_1, \varphi_2\rangle$.

Mostraremos que o conjunto das órbitas do grupo $\langle\varphi_1,\varphi_2\rangle$ é exatamente Bsets($\mathcal{A}$).

Seja $T$ um conjunto básico de $\mathcal{A}$. Se $T=\{k\}$ para algum $k$ em $K$ então $T$ é exatamente a $\langle\varphi_1,\varphi_2\rangle$-órbita de $k$ uma vez que $k^{\varphi_1\varphi_2}=k$. Agora, se $T=Ks$ para algum $s\in H\setminus K$ vamos mostrar que $T$ é a $\langle\varphi_1,\varphi_2\rangle$-órbita de um elemento qualquer de $T$. De fato, basta mostrar esta afirmação para os elementos da base, isto é, basta mostrar nos casos em que $T=Kx$ e $T=Ky$.

- **Caso 1:** $T=Kx$

  Seja $\alpha$ um elemento de $T$. Assim existe $k_1$ em $K$ tal que $\alpha=k_1x$ logo $\alpha^{\varphi_1\varphi_2}=k_1x^{\varphi_1\varphi_2}=k_1xk=k_2x\in T$. Por outro lado, dado $\tilde{k}x$ em $T$ existem $c_1,c_2$ em $\mathbb{F}_p$ tais que $k_1=c_1k$ e $\tilde{k}=c_2k$. Tomando $c=c_2-c_1$ temos $(k_1x)^{\varphi_1^c}=\tilde{k}x$. Portanto $T$ é exatamente a $\langle\varphi_1,\varphi_2\rangle$-órbita de $\alpha$.

- **Caso 2:** $T=Ky$

  Seja $\beta$ um elemento de $T$. Existe $\bar{k}$ em $K$ tal que $\beta=\bar{k}y$ logo $\beta^{\varphi_1\varphi_2}=\bar{k}y^{\varphi_1,\varphi_2}=\bar{k}yk=k'y\in T$. Por outro lado, dado $k_1y$ em $T$ existem $c_1,c_2$ em $\mathbb{F}_p$ tais que $\bar{k}=c_1k$ e $k_1=c_2k$. Tomando $c=c_2-c_1$ temos $(\bar{k}y)^{\varphi_2^c}=k_1y$. Portanto $T$ é exatamente a $\langle\varphi_1,\varphi_2\rangle$-órbita de $\beta$.

Analogamente mostra-se que toda órbita do grupo $\langle\varphi_1,\varphi_2\rangle$ é um conjunto básico de $\mathcal{A}$. Com isso, $\mathcal{A}=V(H,\langle\varphi_1,\varphi_2\rangle)$. ■

Antes do nosso próximo Lema, precisamos de alguns conceitos.

**Definição 4.1.11.** *Uma função $g\colon\mathbb{F}_p\longrightarrow\mathbb{F}_p$ diz-se* **função planar** *se para todo $d$ em $\mathbb{F}_p^*$ a função $g(x+d)-g(x)$ é uma função bijetora.*

A partir disto, temos a seguinte

**Proposição 4.1.12.** *Sejam $\mathbb{F}_p$ um corpo finito com $p$ elementos e $g\colon \mathbb{F}_p \longrightarrow \mathbb{F}_p$ uma função planar. Então $p \geqslant 3$.*

**Demonstração.** Como $g$ é uma função planar então a equação $g(x+d) - g(x) = y$ tem uma solução $x_0$. Se $car\mathbb{F}_p = 2$ então $d + x_0$ é uma outra solução diferente de $x_0$ o que é impossível. ■

Além disso, temos o seguinte

**Teorema 4.1.13.** *Seja $\mathbb{F}_p$ um corpo finito. Toda função planar sobre $\mathbb{F}_p$ é um polinômio quadrático.*

Gluck em [2] , Hiramine em [5] e Rónyai e Szönyi em [10] provaram esse Teorema independentemente. Não colocaremos a demonstração aqui pois nos distanciaríamos dos objetivos desta dissertação.

Para terminarmos a prova do Teorema 4.1.6 falta considerar o caso que existe um conjunto básico $T$ de $\mathcal{A}$ com cardinalidade $p$ e $\mathrm{St}(T) = 1$. Vamos suprir tal caso com o seguinte

**Lema 4.1.14.** *Se $\mathrm{St}(T) = 1$ para algum conjunto básico $T$ de $\mathcal{A}$ com cardinalidade $p$ então $\mathcal{A}$ é Schuriano.*

**Demonstração.** Seja $T$ um conjunto básico de $\mathcal{A}$ tal que $\mathrm{St}(T) = 1$ e $|T| = p$. Pelas Proposições 3.2.17 e 3.2.18 temos que o conjunto $T^{(i)}k$ é um conjunto básico de $\mathcal{A}$ com cardinalidade $p$ para $1 \leqslant i \leqslant p-1$ e $k \in K$. Vamos agora provar algumas afirmações que serão usadas para concluir a demonstração deste Lema.

*Afirmação :* Se $T^{(i_1)}k_1 = T^{(i_2)}k_2$ então $i_1 = i_2$ e $k_1 = k_2$.

Suponhamos que $k_1 \neq k_2$. Se $\mathrm{St}(T^{(i_1)}) \neq 1$ então $\mathrm{St}(T^{(i_1)}) = K$ resultando que $T^{(i_1)}k_1 = T^{(i_1)}k_2$, uma contradição, pois $T^{(i_1)}k_1$ e $T^{(i_1)}k_2$ são conjuntos básicos de $\mathcal{A}$ logo $\mathrm{St}(T^{(i_1)}) = 1$. Além disto, $i_1 \neq i_2$ pois senão teríamos $T^{(i_1)}k = T^{(i_2)}k$, para todo $k \in K$. Agora sejam $i = i_2^{-1}i_1, k = k_1k_2^{-1}$ e seja $l$ a ordem de $i$ em $\mathbb{F}_p^*$. Para todo $t$ em $T$, tem-se que $t^{i_2}k_2 \in T^{(i_2)}k_2 = T^{(i_1)}k_1$; portanto existe $\tilde{t}$ em $T$ tal que $t^{i_2}k_2 = \tilde{t}^{i_1}k_1$.

Isso nos mostra que $t = (\tilde{t}^{i_1}k_1k_2^{-1})^{i_2^{-1}} = (\tilde{t}^{i_1 i_2^{-1}})(k_1k_2^{-1})^{i_2^{-1}} = \tilde{t}^i k^{i_2^{-1}}$. Podemos concluir então que $t \in T^{(i)}k^{i_2^{-1}}$ com $|T| = p = |T^{(i)}k^{i_2^{-1}}|$ portanto $T^{(i)}k^{i_2^{-1}} = T$.

Considere a permutação $\varphi \in \mathrm{Sym}(T)$ definida por $t^\varphi = t^i k^{i_2^{-1}}$. Se $t$ é um elemento de $T$ então a $\varphi$-órbita contendo $t$, isto é, o conjunto $\{t^{\varphi^j} \mid j \in \mathbb{Z}\}$ possui exatamente $l$ elementos a saber $t, t^i k^{i_2^{-1}}, \ldots, t^{i^{l-1}} k^{i_2^{-1}(i^{l-2}+\ldots+i+1)}$ o que nos mostra que toda $\varphi$-órbita possui cardinalidade divisível por $l$, ou seja, $l$ divide $|T| = p$, uma contradição. Conclusão $i_1 = i_2$, o que prova nossa primeira afirmação.

*Afirmação :* Temos que

$$\mathrm{Bsets}(\mathcal{A}) = \{\{k\} \mid k \in K\} \cup \{Kx^i \mid i = 1, \ldots, p-1\} \cup \{T^{(i)}k \mid i = 1, \ldots, p-1, k \in K\}$$

para algum $x$ em $H$.

A Afirmação anterior nos mostra que existem $p^3 - p^2$ elementos de $H$ em $\{T^{(i)}k \mid i = 1, \ldots, p-1, k \in K\}$. Assim existem $S_1, \ldots, S_{p-1}, p-1$ conjuntos básicos de $\mathcal{A}$ com $|S_j| = p, 1 \leqslant j \leqslant p-1$. Agora, se para algum índice $j$ tem-se que $\mathrm{St}(S_j) = 1$ então o conjunto $\{S_j k \mid k \in K\}$ é um conjunto básico de $\mathcal{A}$. Além disto, se $S_j k_1 = T^{(i)}k_2$ temos $S_j \cap T^{(i)}k_3 \neq \emptyset$, logo $\{S_j k \mid k \in K\} \cap \{T^{(i)}k \mid i = 1, \ldots, p-1, k \in K\} = \emptyset$.

Desta maneira, somando as cardinalidades dos conjuntos básicos de $\mathcal{A}$ temos $p^3 - p^2 + p^2 + p^2 - 2p + p = p^3 + p^2 - p > p^3$ uma contradição. Portanto para todo $j$ tem-se que $\mathrm{St}(S_j) = K$ implicando que existe $x \in H \setminus K$ tal que o conjunto $Kx$ é um conjunto básico de $\mathcal{A}$. Mas pela Proposição 3.2.17, o conjunto $Kx^i$ é um conjunto básico de $\mathcal{A}$ para todo $1 \leqslant i \leqslant p-1$ donde concluímos esta afirmação.

Note que $L = \bigcup_{i=0}^{p-1} Kx^i$ é um $\mathcal{A}$-subgrupo de ordem $p^2$.

*Afirmação :* Existem $t_1, t_2$ em $T$ e $l \in L \setminus K$ tal que $t_1 = t_2 l$.

Primeiramente, considere o subconjunto $TL$ de $H$. Sabemos que $1 \notin TL$ pois senão $T \cap L \neq \emptyset$. Com isso concluímos que $TL \subsetneqq H$; logo existem $t_1, t_2 \in T$, $l_1, l_2 \in L$ com $l_1 \neq l_2$ tais que $t_1 l_1 = t_2 l_2$, pois se os elementos de $TL$ fossem distintos teríamos que $|TL| = p^3$ implicando $TL = H$. Assim $t_1 = t_2(l_2 l_1^{-1})$ e o elemento $l_2 l_1^{-1}$ não pertence

a $K$ pois, senão , $t_1$ pertenceria a $T(l_2l_1^{-1}) \cap T$ implicando que $T = T(l_2l_1^{-1})$, isto é, $l_2l_1^{-1} \neq 1 \in \mathrm{St}(T)$ uma contradição. Portanto $l_2l_1^{-1} \in L \setminus K$.

*Afirmação :* Para todo $t$ em $T$ existe um único $f_t$ em $K$ tal que $tl^{-1}f_t^{-1} \in T$.

Existem um índice $i, 1 \leqslant i \leqslant p-1$, e um elemento $k \in K$ tais que $l = kx^i$. Assim $Kl = Kx^i$ pois $x^il^{-1} \in K$. Com isso, sabemos que $\widehat{T}$ e $\widehat{Kl}$ pertencem a $\mathcal{A}$. Mas $\mathcal{A}$ é um espaço vetorial gerado pelo conjunto $\{\widehat{U} \mid U \in \mathrm{Bsets}(\mathcal{A})\}$; logo $\widehat{T}\widehat{Kl} = \sum_{U \in \mathrm{Bsets}(\mathcal{A})} c_U\widehat{U}$. Além disso, sendo $\mathcal{A}$ um S-anel temos $c_T = c_t$ para todo $t \in T$ e, pelo Lema 3.1.3, tem-se que $c_t = |T \cap t[Kl]^{(-1)}|$. A Afirmação anterior nos mostra que $c_T \geqslant 1$ mas, se existem $x_1, x_2$ em $T$ e $k_1, k_2$ em $K$ com $x_1(k_1l) = x_2(k_2l)$, então o elemento $k_1k_2^{-1}$ estabiliza $T$; portanto $k_1 = k_2$ e $x_1 = x_2$. Isto prova que $c_T = 1$ e, em particular, para todo $t$ em $T$ existe um único $f_t$ em $K$ tal que $tl^{-1}f_t^{-1} \in T$ o que encerra a demonstração desta afirmação .

Fixemos um base $\{e_1, e_2, e_3\}$ de $H$ satisfazendo $e_1 \in T, e_2 = (lf_{e_1})^{-1}$ e $K = \langle e_3 \rangle$.

*Afirmação :* $T = \{e_1(ie_2)(f(i)e_3) \mid 0 \leqslant i \leqslant p-1\}$ para alguma função $f\colon \mathbb{F}_p \longrightarrow \mathbb{F}_p$ tal que $0^f = 0$ e $1^f = 0$.

Sabemos que, como $f_{e_1} \in K$, existe um único $\bar{c}$ em $\mathbb{F}_p$ tal que $f_{e_1} = \bar{c}e_3$. Vamos mostrar que se $e_1(ie_2)(f(i)e_3)$ pertence a $T$ para algum $f(i) \in \mathbb{F}_p$, então existe $f(i+1) \in \mathbb{F}_p$ satisfazendo $e_1((i+1)e_2)(f(i+1)e_3) \in T$.

Se $i = 0$, como $e_1 \in T$, podemos tomar $0^f = 0$. Suponhamos que $e_1(ie_2)(f(i)e_3)$ pertence a $T$ para algum $f(i) \in \mathbb{F}_p$, então pela Afirmação anterior, existe um único $\tilde{c}$ em $\mathbb{F}_p$ tal que $e_1(ie_2)(f(i)e_3)l^{-1}(\tilde{c}e_3)^{-1} \in T$, equivalentemente,

$$e_1(ie_2)(f(i)e_3)e_2\bar{c}e_3(\tilde{c}e_3)^{-1} = e_1((i+1)e_2)((f(i)+c)e_3) \in T$$

onde $c = \bar{c} - \tilde{c}$. Assim podemos definir $f(i+1) = f(i) + c$.

O conjunto $\{e_1(ie_2)(f(i)e_3) \mid i \in \mathbb{F}_p\}$ tem cardinalidade $p$ e está contido em $T$ portanto $\{e_1(ie_2)(f(i)e_3) \mid i \in \mathbb{F}_p\} = T$. Por fim, como $e_1(0e_2)(f(0)e_3) = e_1 \in T$, pela Afirmação anterior, existe um único $c_1$ em $\mathbb{F}_p$ tal que $e_1e_2(f(0)+c_1)e_3 = e_1e_2(c_1e_3) \in T$.

Mas $e_1 l^{-1} f_{e_1}^{-1} = e_1 e_2 \in T$, logo $c_1 = 0$, implicando que $1^f = 0$.

*Afirmação :* Para todo $k \in \mathbb{F}_p \setminus \{0\}$ temos que $\{f(i) - f(i-k) \mid i \in \mathbb{F}_p\} = \mathbb{F}_p$. Em particular podemos assumir que $2^f = 1$.

Usando a descrição do conjunto $T$, temos que

$$\widehat{T}\widehat{T^{(-1)}} = p1 + \sum_{k=0}^{p-1} \widehat{K(ke_2)}$$

Em particular, para todo $k \neq 0$, o conjunto

$$\{(e_1 i e_2 f(i) e_3)(e_1(i-k) e_2 f(i-k) e_3)^{-1} \mid i \in \mathbb{F}_p\}$$

é um subconjunto de $K(ke_2)$ com cardinalidade $p$ logo,

$$\{(e_1 i e_2 f(i) e_3)(e_1(i-k) e_2 f(i-k) e_3)^{-1} \mid i \in \mathbb{F}_p\} = K(ke_2).$$

Por fim, para todo $k \in \mathbb{F}_p \setminus \{0\}$ o conjunto $\{f(i) - f(i-k) \mid i \in \mathbb{F}_p\}$ é um subconjunto de $\mathbb{F}_p$ contendo $p$ elementos. De fato, se $f(i) - f(i-k) = f(j) - f(j-k)$ para $i, j \in \mathbb{F}_p$ com $i \neq j$ então $(e_1 i e_2 f(i) e_3)(e_1(i-k) e_2 f(i-k) e_3)^{-1} = (e_1 j e_2 f(j) e_3)(e_1(j-k) e_2 f(j-k) e_3)^{-1}$ o que nos diz que $|K(ke_2)| = p - 1$ mas isto é uma contradição .

Note que $2^f$ não pode ser 0 uma vez que sendo $0^f = 1^f = 0$ teremos $\{f(i) - f(i-k) \mid i \in \mathbb{F}_p\} \subset \mathbb{F}_p$. Assim, sem perda de generalidade, podemos assumir que $2^f = 1$ fazendo a mudança da base $\{e_1, e_2, e_3\}$ para a base $\{e_1, e_2, (2^f)^{-1} e_3\}$.

A próxima afirmação determina exatamente a nossa função $f$.

*Afirmação :* $f(x) = (x^2 - x)/2$

Pelo Teorema 4.1.13, sabemos que existem $a, b, c \in \mathbb{F}_p$ tais que $f(x) = ax^2 + bx + c$. Mas $0^f = 1^f = 0$ e $2^f = 1$ logo $f(x) = (x^2 - x)/2$.

Estamos prontos para terminar a demonstração do Lema 4.1.14. Para isto, seja $\varphi \in \mathrm{GL}(H)$ definida por

$$\varphi : \begin{array}{l} e_1 \longmapsto e_1e_2 \\ e_2 \longmapsto e_2e_3 \\ e_3 \longmapsto e_3 \end{array}$$

Considere o grupo de permutações $G = R_H \rtimes \langle\varphi\rangle$.

*Afirmação :* O conjunto das órbitas do grupo $\langle\varphi\rangle$ é exatamente $\mathrm{Bsets}(\mathcal{A})$.

Inicialmente vamos mostrar que $G_1 = \langle\varphi\rangle$. De fato, como $e_3^{\varphi} = e_3$ e $1 \in K$ então $1^{\varphi} = 1$, ou seja, $\varphi \in G_1$. Por outro lado, seja $f \in G_1$ existem $\varphi^j \in \langle\varphi\rangle$ e $R_h \in R_H$ tais que $f = \varphi^j R_h$. Assim $1^f = 1^{\varphi^j R_h} = 1^{R_h} = h = 1$ logo $f \in \langle\varphi\rangle$. Vamos agora demonstrar a Afirmação . Para isto, seja $\bar{T}$ um conjunto básico de $\mathcal{A}$.

- **Caso 1:** $\bar{T} = \{k\}$ para algum $k$ em $K$.

  Existe $\bar{c} \in \mathbb{F}_p$ com $k = \bar{c}e_3$. Portanto $k^{\varphi} = \bar{c}e_3^{\varphi} = \bar{c}e_3 = k$. Logo, para todo $\varphi^j$, $k^{\varphi^j} = k$. Isto nos mostra que $\bar{T}$ é a $\langle\varphi\rangle$-órbita de $k$.

- **Caso 2:** $\bar{T} = Kx^i$ para algum $i \in \{1, \ldots, p-1\}$.

  Sabemos que existem $\alpha_1, \alpha_2, \alpha_3$ em $\mathbb{F}_p$ tais que $x = \alpha_1e_1\alpha_2e_2\alpha_3e_3$. Dado $kx^i$ em $\bar{T}$ vamos mostrar que $(kx^i)^{\varphi} \in \bar{T}$. Note que para isto ocorrer é suficiente mostrar que $(x^i)^{\varphi} \in \bar{T}$. De fato,

  $$\begin{aligned}(x^i)^{\varphi} &= [(\alpha_1e_1\alpha_2e_2\alpha_3e_3)^{\varphi}]^i \\ &= (\alpha_1(e_1e_2)\alpha_2(e_2e_3)\alpha_3e_3)^i \\ &= (\alpha_1e_1)^i(\alpha_2e_2)^i(\alpha_3e_3)^i(\alpha_1e_2)^i(\alpha_2e_3)^i \\ &= x^i(\alpha_1e_2)^i(\alpha_2e_3)^i\end{aligned}$$

  Suponhamos, por absurdo, que $(x^i)^{\varphi} \notin \bar{T}$. Sabemos que $(x^i)^{\varphi} \notin K$ pois senão $x^i = [(x^i)^{\varphi}]^{\varphi^{-1}} = (x^i)^{\varphi} \in K$. Se $(x^i)^{\varphi} \in Kx^j$ então $x^i(\alpha_1e_2)^i(\alpha_2e_3)^i = k_1x^j$ implicando que $(\alpha_1e_2)^i = k_2x^{(j-i)}$, ou seja, $(\alpha_1e_1)^{(j-i)}(\alpha_2e_2)^{(j-i)}((\alpha_3+c)e_3)^{(j-i)} = (\alpha_1e_2)^i$ logo $(j-i)\alpha_1 = 0$, isto é, $j = i$. Agora, temos que $e_2 \in L$ logo $(\alpha_1e_2)^i \in L$.

Além disso, $x^i \in L$ portanto $x^i(\alpha_1 e_2)^i \in L$. Assim, se $(x^i)^\varphi \in T^{(s)}k_1$ então $x^i(\alpha_1 e_2)^i(\alpha_2 e_3)^i = t^s k_1$, ou seja, $x^i(\alpha_1 e_2)^i \in T^{(s)}k_2$ uma contradição pois $L \cap T^{(s)}k_2 = \emptyset$. Consequentemente, concluímos que $(x^i)^\varphi \in Kx^i$; portanto, a $\langle\varphi\rangle$-órbita do elemento $kx^i$ está contida em $Kx^i$.

Note que existem $\bar{c}, c$ em $\mathbb{F}_p$ tais que $(ce_3x^i)^\varphi = ce_3\bar{c}e_3x^i = (c+\bar{c})e_3x^i$. Com isso, $(ce_3x^i)^{\varphi^2} = (c+2\bar{c})e_3x^i$ e assim $(ce_3x^i)^{\varphi^j} = (c+j\bar{c})e_3x^i$. Por fim, dado $\tilde{k}x^i$ um elemento qualquer de $Kx^i$ existe $\tilde{c}$ em $\mathbb{F}_p$ tal que $\tilde{k} = \tilde{c}e_3$. Tomando $j = (\tilde{c}-c)/\bar{c}$ temos $(kx^i)^{\varphi^j} = (ce_3x^i)^{\varphi^j} = (c+j\bar{c})e_3x^i = \tilde{c}e_3 = \tilde{k}x^i$. Consequentemente, a $\langle\varphi\rangle$-órbita de $kx^i$ é exatamente $Kx^i = \bar{T}$.

- **Caso 3:** $\bar{T} = T^{(s)}k$ para algum $s, 1 \leqslant s \leqslant p-1, k \in K$.
  Seja $t^sk$ um elemento de $\bar{T}$. Como $t \in T$ existe $j \in \mathbb{F}_p$ satisfazendo $t = e_1je_2f(j)e_3$. Assim

$$\begin{aligned}(t^sk)^\varphi = (t^s)^\varphi k &= (e_1^s)^\varphi((je_2)^s)^\varphi((f(j)e_3)^s)^\varphi k\\ &= (e_1e_2)^s(j(e_2e_3))^s(f(j)e_3)^s k\\ &= e_1^s(je_2)^s(f(j)e_3)^s e_2^s(je_3)^s k\\ &= e_1^s((j+1)e_2)^s(f(j)+j)e_3)^s k.\end{aligned}$$

  Mas $f(j+1) - f(j) = (-j^2+j)/2 + (j^2+2j+1-j-1)/2 = j$ portanto $(t^sk)^\varphi = (e_1(j+1)e_2(f(j+1)e_3)^s k \in T^{(s)}k$. Podemos concluir que $(t^sk)^{\varphi^l} \in T^{(s)}k$ para todo índice $l, 1 \leqslant l \leqslant o(\varphi)$ e isto implica que a $\langle\varphi\rangle$-órbita do elemento $t^sk$ está contida em $T^{(s)}k$. Por outro lado, dado $\tilde{t}^sk$ um elemento qualquer de $T^{(s)}k$, existe $\tilde{j} \in \mathbb{F}_p$ com $\tilde{t} = e_1\tilde{j}e_2f(\tilde{j})e_3$. Tomando $l = \tilde{j} - j$ temos

  $((e_1je_2f(j)e_3)^s k)^{\varphi^l} = (e_1(j+\tilde{j}-j)e_2f(j+\tilde{j}-j)e_3)^s k = (e_1\tilde{j}e_2f(\tilde{j})e_3)^s k = \tilde{t}^s k.$
  Portanto o conjunto $T^{(s)}k$ está contido na $\langle\varphi\rangle$-órbita do elemento $t^sk$. Assim concluímos que a $\langle\varphi\rangle$-órbita do elemento $t^sk$ é exatamente o conjunto $T^{(s)}k$.

Acabamos de mostrar que todo conjunto básico de $\mathcal{A}$ é uma órbita do grupo $G_1 = \langle\varphi\rangle$. Analogamente mostra-se que toda órbita do grupo $\langle\varphi\rangle$ é um conjunto básico de $\mathcal{A}$. Com isso finalizamos a Afirmação, o Lema 4.1.14 e o Teorema 4.1.6. ■

# Capítulo 5

# Isomorfismos entre S-anéis

O desenvolvimento do conteúdo deste capítulo não está diretamente relacionado com os resultados desenvolvidos no capítulo 4 , mas estão incluídos aqui com o objetivo de enriquecer o trabalho.

## 5.1 Definições e Propriedades

**Definição 5.1.1.** *Sejam $\mathcal{A} \subseteq \mathbb{Q}H$ e $\mathcal{B} \subseteq \mathbb{Q}K$ dois S-anéis sobre os grupos $H$ e $K$ respectivamente. Uma função $\varphi\colon \mathcal{A} \longrightarrow \mathcal{B}$ diz-se um* **S-isomorfismo** *se é um isomorfismo de $\mathbb{Q}$-álgebras e $(B_S(\mathcal{A}))^{\varphi} = B_S(\mathcal{B})$ onde $B_S(\mathcal{A}) = \{\widehat{T} \mid T \in \mathrm{Bsets}(\mathcal{A})\}$ e $B_S(\mathcal{B}) = \{\widehat{T} \mid T \in \mathrm{Bsets}(\mathcal{B})\}$. Uma bijeção $f\colon \mathrm{Bsets}(\mathcal{A}) \longrightarrow \mathrm{Bsets}(\mathcal{B})$ diz-se um* **S-isomorfismo de conjuntos básicos** *se induz por linearidade um* **S-isomorfismo** *entre $\mathcal{A}$ e $\mathcal{B}$, ou seja, se aplicação $\sum_i a_i\widehat{T_i} \longrightarrow \sum_i a_i\widehat{T_i^f}$ é um* **S-isomorfismo** *entre $\mathcal{A}$ e $\mathcal{B}$.*

**Definição 5.1.2.** *Sejam $\mathcal{A} \subseteq \mathbb{Q}H$ e $\mathcal{B} \subseteq \mathbb{Q}K$ dois S-anéis sobre os grupos $H$ e $K$ respectivamente. Uma aplicação bijetora $f\colon H \longrightarrow K$ diz-se um* **isomorfismo combinatório de S-anéis** *se para cada* T *pertencente à* Bsets$(\mathcal{A})$ *existe* S *pertencente à* Bsets$(\mathcal{B})$ *tal que* Cay$(H,T)^f$=Cay$(K,S)$, *ou equivalentemente, dados $x, y \in H$ então $xy^{-1}$ pertence à* T *se e somente se $x^f(y^f)^{-1}$ pertence à* S.

*Além disso,* $f\colon H \longrightarrow K$ *diz-se um* **isomorfismo de Cayley de S-anéis** *se for um isomorfismo de grupos e um* **isomorfismo combinatório de S-anéis**.

Note que todo isomorfismo de Cayley de S-anéis é um isomorfismo combinatório de S-anéis mas em geral a recíproca é falsa. Denotamos $\mathcal{A} \cong_{\text{Cay}} \mathcal{B}$ ($\mathcal{A} \cong_{com} \mathcal{B}$) se existe um isomorfismo de Cayley (combinatório) entre $\mathcal{A}$ e $\mathcal{B}$.

**Proposição 5.1.3.** *Sejam* $\mathcal{A} \subseteq \mathbb{Q}H$ *e* $\mathcal{B} \subseteq \mathbb{Q}K$ *dois S-anéis sobre os grupos* $H$ *e* $K$ *respectivamente. Se* $f\colon H \longrightarrow K$ *é um isomorfismo combinatório de S-anéis então, para cada elemento* $k \in K$, *o produto* $fR_k\colon H \longrightarrow K$ *também é um isomorfismo combinatório de S-anéis.*

**Demonstração.** Seja $f\colon H \longrightarrow K$ um isomorfismo combinatório entre $\mathcal{A}$ e $\mathcal{B}$. Para cada $T \in \text{Bsets}(\mathcal{A})$ existe $S \in \text{Bsets}(\mathcal{B})$ tal que $\text{Cay}(H,T)^f = \text{Cay}(K,S)$. Vamos mostrar que $\text{Cay}(H,T)^{fR_k} = \text{Cay}(K,S)$. De fato, se $z \in \text{Cay}(H,T)^{fR_k}$ então $z = (x^{fR_k}, y^{fR_k})$ com $(x,y) \in \text{Cay}(H,T)$. Mas $x^{fR_k}(y^{fR_k})^{-1} = (x^f k)(y^f k)^{-1} = x^f(y^f)^{-1} \in S$ consequentemente $z \in \text{Cay}(K,S)$. Por outro lado, se $w \in \text{Cay}(K,S)$ existem $x, y \in H$ tais que $w = (x^{fR_k}, y^{fR_k})$ e $x^{fR_k}(y^{fR_k})^{-1} = (x^f k)(y^f k)^{-1} = x^f(y^f)^{-1} \in S$ portanto $(x^f, y^f) \in \text{Cay}(K,S) = \text{Cay}(H,T)^f$ implicando que $xy^{-1} \in T$ logo $w \in \text{Cay}(H,T)^{fR_k}$ donde segue a tese. ■

Agora, se $\mathcal{A} \subseteq \mathbb{Q}H$ e $\mathcal{B} \subseteq \mathbb{Q}K$ são dois S-anéis sobre os grupos $H$ e $K$ respectivamente e $f\colon H \longrightarrow K$ é um isomorfismo combinatório de S-anéis, a Proposição 5.1.3 garante que tomando $k = (1_H^f)^{-1}$ e multiplicando $f$ por $R_k$, tem-se que $fR_k$ é um isomorfismo combinatório de S-anéis com a propriedade que $1_H^{fR_k} = 1_K$. Isto nos motiva a introduzir a seguinte

**Definição 5.1.4.** *Sejam* $\mathcal{A} \subseteq \mathbb{Q}H$ *e* $\mathcal{B} \subseteq \mathbb{Q}K$ *dois S-anéis sobre os grupos* $H$ *e* $K$ *respectivamente. Um isomorfismo combinatório* $f\colon H \longrightarrow K$ *de S-anéis diz-se* **isomorfismo combinatório normalizado** *se* $1_H^f = 1_K$.

A seguir damos um resultado que nos ajudará a mostrar que todo isomorfismo combinatório de S-anéis induz um S-isomorfismo.

**Lema 5.1.5.** *Sejam $\mathcal{A} \subseteq \mathbb{Q}H$ e $\mathcal{B} \subseteq \mathbb{Q}K$ dois S-anéis sobre os grupos $H$ e $K$ respectivamente. Suponhamos que $\mathcal{A}$ e $\mathcal{B}$ sejam combinatoriamente isomorfos e considere $f\colon H \longrightarrow K$ um isomorfismo combinatório entre $\mathcal{A}$ e $\mathcal{B}$. Se $f$ for normalizado então para todo* T *em* Bsets*($\mathcal{A}$) existe* S *em* Bsets*($\mathcal{B}$) tal que $T^f = S$.*

**Demonstração.** Seja $T$ pertencente à Bsets($\mathcal{A}$). Por hipótese, existe $S$ em Bsets($\mathcal{B}$) tal que $\mathrm{Cay}(H,T)^f$=$\mathrm{Cay}(K,S)$. Assim, dado $x \in T$ temos $(x,1) \in \mathrm{Cay}(H,T)$ implicando que $(x^f, 1^f) \in \mathrm{Cay}(K,S)$ e portanto $x^f \in S$. Segue que $T^f \subseteq S$. Por outro lado, se $y \in S$, existe um único $x \in H$ tal que $y = x^f$. Com isso, temos que $(y,1) = (x^f, 1^f) \in \mathrm{Cay}(K,S)$=$\mathrm{Cay}(H,T)^f$; logo $(x,1) \in \mathrm{Cay}(H,T)$. Deste fato, podemos concluir que $x \in T$ e $T^f = S$. ■

**Observação 5.1.6.** O Lema 5.1.5 nos permite concluir que se $f\colon H \longrightarrow K$ é um isomorfismo combinatório normalizado entre os S-anéis $\mathcal{A} \subseteq \mathbb{Q}H$ e $\mathcal{B} \subseteq \mathbb{Q}K$, então $\big(\mathrm{Bsets}(\mathcal{A})\big)^f = \mathrm{Bsets}(\mathcal{B})$.

**Proposição 5.1.7.** *Sejam $\mathcal{A} \subseteq \mathbb{Q}H$ e $\mathcal{B} \subseteq \mathbb{Q}K$ dois S-anéis sobre os grupos $H$ e $K$ respectivamente. Se uma dada bijeção $f\colon H \longrightarrow K$ tal que $1^f = 1$ é um isomorfismo combinatório normalizado de S-anéis, então para cada $T$ em* Bsets*($\mathcal{A}$) e x,y em $H$ são equivalentes:*

*(i)* $xy^{-1} \in T$

*(ii)* $x^f(y^f)^{-1} \in T^f$

**Demonstração.** Se $f$ é um isomorfismo combinatório, pelo Lema 5.1.5, para cada $T$ em Bsets($\mathcal{A}$) existe $S$ em Bsets($\mathcal{B}$) tal que $T^f = S$. Além disso, $\mathrm{Cay}(K,S)$=$\mathrm{Cay}(H,T)^f$. Assim $xy^{-1} \in T \Leftrightarrow (x,y) \in \mathrm{Cay}(H,T)$

$$\Leftrightarrow (x^f, y^f) \in \mathrm{Cay}(H,T)^f = \mathrm{Cay}(K,T^f)$$

$$\Leftrightarrow x^f(y^f)^{-1} \in T^f.$$ ■

Considere $\mathcal{A} \subseteq \mathbb{Q}H$ e $\mathcal{B} \subseteq \mathbb{Q}K$ dois S-anéis sobre os grupos $H$ e $K$ respectivamente. Suponhamos que $\mathcal{A}$ e $\mathcal{B}$ sejam combinatoriamente isomorfos e considere $f\colon H \longrightarrow K$ um isomorfismo combinatório entre $\mathcal{A}$ e $\mathcal{B}$. Tomando $k = (1^f)^{-1}$, a Proposição 5.1.3 garante que a função $fR_k\colon H \longrightarrow K$ é um isomorfismo combinatório normalizado entre $\mathcal{A}$ e $\mathcal{B}$. Denotaremos $g = fR_k$. Assim, para cada $T$ em Bsets($\mathcal{A}$) existe $S$ em Bsets($\mathcal{B}$) satisfazendo Cay$(H,T)^g$=Cay$(K,S)$ e $T^g = S$. Por esta razão , $g$ induz uma bijeção $g^*\colon$ Bsets($\mathcal{A}$) $\longrightarrow$ Bsets($\mathcal{B}$) tal que Cay$(H,T)^g$=Cay$(K,T^{g^*})$.

**Proposição 5.1.8.** *A função $g^*$ é um S-isomorfismo de conjuntos básicos entre $\mathcal{A}$ e $\mathcal{B}$.*

**Demonstração.** Primeiro, considere Bsets($\mathcal{A}$)= $\{T_0, \ldots, T_d\}$ e Bsets($\mathcal{B}$) = $\{S_0, \ldots, S_d\}$. Devemos mostrar que $g^*$ induz por linearidade um S-isomorfismo. Mais explicitamente, devemos mostrar que a função $\varphi\colon \mathcal{A} \longrightarrow \mathcal{B}$ dada por: $\left(\widehat{T}\right)^{\varphi} = \widehat{T^{g^*}} = \widehat{T^g}$ é um S-isomorfismo.

De fato, dados $T_i, T_j$ em Bsets($\mathcal{A}$) existem $S_l, S_t$ em Bsets($\mathcal{B}$) tais que $T_i^g = S_l$ e $T_j^g = S_t$. Desta maneira, $\widehat{T_i}\widehat{T_j} = \sum_{k=0}^{d} \alpha_k \widehat{T_k}$ implicando que

$$(\widehat{T_i}\widehat{T_j})^{\varphi} = \sum_{k=0}^{d} \alpha_k (\widehat{T_k})^{\varphi} = \sum_{k=0}^{d} \alpha_k \widehat{T_k^g}$$

e

$$\widehat{S_l}\widehat{S_t} = \sum_{m=0}^{d} \beta_m \widehat{S_m}.$$

*Afirmação:* Para cada índice $k$, $0 \leqslant k \leqslant d$, existe um índice $m$, $0 \leqslant m \leqslant d$, que satisfaz $\alpha_k = \beta_m$.

Seja $t_0 \in T_k$. Pelo Lema 3.1.3, $\alpha_k = \theta_{t_0}(\widehat{T_i}, \widehat{T_j}) = |T_i \cap t_0 T_j^{(-1)}|$. Mas como $g$ é um isomorfismo combinatório normalizado, existe $m, 0 \leqslant m \leqslant d$, com $T_k^g = S_m$ garantindo que $t_0^g \in S_m$. Além disso, $\beta_m = \theta_{t_0^g}(\widehat{S_l}, \widehat{S_t}) = |S_l \cap t_0^g S_t^{(-1)}|$. Por fim, a função

$$\psi\colon T_i \cap t_0 T_j^{(-1)} \longrightarrow S_l \cap t_0^g S_t^{(-1)}$$

$$t_0 y^{-1} \longmapsto t_0^g (y^g)^{-1}$$

é uma bijeção. Deste fato concluímos que $\alpha_k = \beta_m$ o que prova a nossa afirmação. Portanto $(\widehat{T_i}\widehat{T_j})^\varphi = (\widehat{T_i})^\varphi(\widehat{T_j})^\varphi$ donde segue que $\varphi$ é um isomorfismo de $\mathbb{Q}$-álgebras. ■

Sejam $\mathcal{A} \subseteq \mathbb{Q}H$ e $\mathcal{B} \subseteq \mathbb{Q}K$ dois S-anéis sobre os grupos $H$ e $K$ respectivamente. A conexão entre os três tipos de isomorfismo é dada pelas seguintes implicações:

$$\mathcal{A} \cong_{\text{Cay}} \mathcal{B} \quad \Rightarrow \quad \mathcal{A} \cong_{com} \mathcal{B} \quad \Rightarrow \quad \mathcal{A} \cong_{\mathbb{Q}} \mathcal{B}$$

Em geral não vale

$$\mathcal{A} \cong_{\text{Cay}} \mathcal{B} \quad \Leftarrow \quad \mathcal{A} \cong_{com} \mathcal{B} \quad \Leftarrow \quad \mathcal{A} \cong_{\mathbb{Q}} \mathcal{B}$$

Para cada S-anel $\mathcal{A} \subseteq \mathbb{Q}H$ podemos associar dois subconjuntos de $\text{Sym}(H)$:
$Iso(\mathcal{A}) = \{f \in \text{Sym}(H) \mid f$ é um iso combinatório de $\mathcal{A}$ em um S-anel sobre $H\}$,
$Iso_1(\mathcal{A}) = \{f \in Iso(\mathcal{A}) \mid 1^f = 1\}$.

Note que se $f \in Iso(\mathcal{A})$ podemos escrever $f$ da forma $f = (f(R_{1^f})^{-1})R_{1^f}$ o que nos permite estabelecer uma relação entre os conjuntos $Iso(\mathcal{A})$ e $Iso_1(\mathcal{A})$. Explicitamente, $Iso(\mathcal{A}) = Iso_1(\mathcal{A})R_H$.

**Proposição 5.1.9.** *Sejam $\mathcal{A} \subseteq \mathbb{Q}H$ e $\mathcal{B} \subseteq \mathbb{Q}K$ dois S-anéis combinatoriamente isomorfos sobre os grupos $H$ e $K$ respectivamente e $f\colon H \longrightarrow K$ um isomorfismo combinatório normalizado de $\mathcal{A}$ em $\mathcal{B}$. Então:*

*i) Se $\widehat{E} \in \mathcal{A}$ para algum subgrupo $E$ de $H$, então $E^f$ é um subgrupo de $K$ e $f_E\colon E \longrightarrow E^f$ é um isomorfismo combinatório de $\mathcal{A}_E$ em $\mathcal{B}_{E^f}$.*

*ii) para cada $h \in H$, temos $(Eh)^f = E^f h^f$.*

*iii) Se $\widehat{E} \in \mathcal{A}$ para algum subgrupo normal $E$ de $H$ tal que $E^f$ é um subgrupo normal de $K$, então a aplicação $f^{H/E}\colon H/E \longrightarrow K/E^f$ definida pela fórmula $(Eh)^{f^{H/E}} = E^f h^f$ é um isomorfismo combinatório normalizado entre $\mathcal{A}/E$ e $\mathcal{B}/E^f$.*

**Demonstração.** *i)* Como $f$ é normalizado, $\text{Cay}(H,T)^f = \text{Cay}(K,T^f)$ para cada $T$ em $\text{Bsets}(\mathcal{A})$. Além disso, $E$ é uma união de conjuntos básicos de $\mathcal{A}$ pois $\widehat{E} \in \mathcal{A}$.

*Afirmação:* $\mathrm{Cay}(H,E)^f = \mathrm{Cay}(K,E^f)$.

Existem $T_{i_1},\ldots,T_{i_s}$ em $\mathrm{Bsets}(\mathcal{A})$ tais que $E=\bigcup_{j=1}^{s} T_{i_j}$ portanto $E^f=\bigcup_{j=0}^{s} T_{i_j}^f$ o que implica $x\in \mathrm{Cay}(H,E)^f \Leftrightarrow x=(z^f,w^f)$ com $zw^{-1}\in T_{i_k}$ para algum $k, 1\leqslant k\leqslant s, \Leftrightarrow$ $x\in \mathrm{Cay}(H,T_{i_k})^f = \mathrm{Cay}(H,T_{i_k}^f) \Leftrightarrow x\in \mathrm{Cay}(H,E^f)$.

Agora, como $E\leqslant H$, o Teorema 2.1.3 nos diz que $\mathrm{Cay}(H,E)$ é uma relação de equivalência em $H$, logo $\mathrm{Cay}(K,E^f)$ é uma relação de equivalência em $K$ e novamente o Teorema 2.1.3 mostra que $E^f\leqslant K$. Por fim, se $T$ pertence a $\mathrm{Bsets}(\mathcal{A}_E)$ então $T$ pertence a $\mathrm{Bsets}(\mathcal{A})$ com $T\subseteq E$. Mas $f$ é um isomorfismo combinatório, ou seja, existe $S$ em $\mathrm{Bsets}(\mathcal{B})$ tal que $T^f=S\subseteq E^f$ mostrando que $T^f$ pertence a $\mathrm{Bsets}(\mathcal{B}_{E^f})$. Concluímos que $f_E\colon E\longrightarrow E^f$ é um isomorfismo combinatório de $\mathcal{A}_E$ em $\mathcal{B}_{E^f}$.

*ii)* Sejam $e\in E, h\in H$ elementos arbitrários e considere o par $(h,eh)\in \mathrm{Cay}(H,E)$. Então $(h^f,(eh)^f)\in \mathrm{Cay}(K,E^f)$, isto é, $h^f[(eh)^f]^{-1}=e_1^f$ para algum $e_1\in E$ o que é equivalente a dizer que $(e_1^f)^{-1}h^f=(eh)^f$. Mas $E^f\leqslant K$ logo $(e_1^f)^{-1}\in E^f$ implicando que $(eh)^f\in E^fh^f$, portanto $(Eh)^f\subseteq E^fh^f$. Por outro lado, $|Eh|=|E|=|E^f|=|E^fh^f|$. Considere $\varphi\colon (Eh)^f\longrightarrow E^f$ dada por $\varphi[(eh)^f]=e^f$. Claramente $\varphi$ é bijetora; consequentemente $|(Eh)^f|=|E^f|$ e $(Eh)^f=E^fh^f$.

*iii)* Inicialmente temos a seguinte função $f^{H/E}\colon H/E\longrightarrow K/E^f$ definida pela fórmula $(Eh)^{f^{H/E}}=E^fh^f$.

- $f^{H/E}$ está bem definida e é bijetora

  De fato, se $Eh_1=Eh_2$ então $(Eh_1)^{f^{H/E}}=E^fh_1^f=(Eh_1)^f=(Eh_2)^f=E^fh_2^f=(Eh_2)^{f^{H/E}}$ mostrando que $f^{H/E}$ está bem definida. Além disso, se $(Eh_1)^{f^{H/E}}=(Eh_2)^{f^{H/E}}$ então $E^fh_1^f=E^fh_2^f$ implicando que $(Eh_1)^f=(Eh_2)^f$ e sendo $f$ bijetora temos $Eh_1=Eh_2$, isto é, $f^{H/E}$ é injetora. Por fim, dado $\alpha\in K/E^f$ existe $h\in H$ tal que $\alpha=E^fh^f=(Eh)^f=(Eh)^{f^{H/E}}$, ou seja, $f^{H/E}$ é sobrejetora.

- Para todo $\bar{T}$ em Bsets$(\mathcal{A}/E)$, Cay$(H/E,\bar{T})^{f^{H/E}}$ = Cay$(K/E^f,\bar{T}^{f^{H/E}})$.

  De fato, dado $\bar{T}$ em Bsets$(\mathcal{A}/E)$, existe $T$ em Bsets$(\mathcal{A})$ tal que $\bar{T} = \{tE \mid t \in T\}$. Vamos denotar o conjunto $\{tE \mid t \in T\}$ por $T/E$. Seja $x$ um elemento do conjunto Cay$(K/E^f,\bar{T}^{f^{H/E}})$ = Cay$(K/E^f,(T/E)^{f^{H/E}})$. Existem $h_1, h_2 \in H$ tais que $x = (E^f h_1^f, E^f h_2^f)$ com $(E^f h_1^f)(E^f h_2^f)^{-1} = E^f h_1^f (h_2^f)^{-1} \in (T/E)^{f^{H/E}}$, ou seja, existe $t \in T$ tal que $E^f h_1^f (h_2^f)^{-1} = (tE)^{f^{H/E}}$. O fato de $E \trianglelefteq H$ implica que $E^f h_1^f (h_2^f)^{-1} = (Et)^{f^{H/E}} = E^f t^f$; logo $h_1^f (h_2^f)^{-1} \in E^f t^f = (Et)^f = (tE)^f$, isto é, existe $e \in E$ com $h_1^f (h_2^f)^{-1} = e^f t^f$. Mas $f$ é um isomorfismo combinatório, portanto $h_1^f (h_2^f)^{-1} (e^f)^{-1} = h_1^f (e^f h_2^f)^{-1} = (h_1^f (e_1 h_2)^f)^{-1}) = t^f$ o que implica $h_1 (e_1 h_2)^{-1} = \tilde{t}$ e $h_1 h_2^{-1} \in \tilde{t}E$. Assim $Eh_1 h_2^{-1} = (Eh_1)(Eh_2)^{-1} \in T/E$. Por fim $x = ((Eh_1)^{f^{H/E}}, (Eh_2)^{f^{H/E}})$ com $Eh_1 h_2^{-1} = (Eh_1)(Eh_2)^{-1} \in T/E$ o que nos mostra que $x \in$ Cay$(H/E,\bar{T})^{f^{H/E}}$.

  Seja agora $y$ um elemento do conjunto Cay$(H/E,\bar{T})^{f^{H/E}}$=Cay$(H/E,T/E)^{f^{H/E}}$. Existem $Eh_1$, $Eh_2$ em $H/E$ com $(Eh_1)(Eh_2)^{-1} \in T/E$ tais que $y = ((Eh_1)^{f^{H/E}}, (Eh_2)^{f^{H/E}}) = (E^f h_1^f, E^f h_2^f)$. Mas o fato de que $(Eh_1)(Eh_2)^{-1} = E(h_1 h_2^{-1}) \in T/E$ implica que $h_1 h_2^{-1} \in tE$ para algum $t \in T$ logo existe $\tilde{t} \in T$ tal que $h_1^f (h_2^f)^{-1} \in (\tilde{t}E)^f$ pois $f$ é um isomorfismo combinatório. Agora, $(\tilde{t}E)^f = (E\tilde{t})^f = E^f \tilde{t}^f$, ou seja, $h_1^f (h_2^f)^{-1} \in (\tilde{t}E)^{f^{H/E}}$. Portanto $E^f h_1^f (h_2^f)^{-1} = (E^f h_1^f)(E^f h_2^f)^{-1} \in (T/E)^{f^{H/E}}$ e, consequentemente $y \in$ Cay$(K/E^f,\bar{T}^{f^{H/E}})$.

- $\bar{T} = (T/E)^{f^{H/E}}$ pertence a Bsets$(\mathcal{B}/E^f)$.

  De fato, seja $T \in$ Bsets$(\mathcal{A})$. Existe $S \in$ Bsets$(\mathcal{B})$ tal que $T^f = S$. Assim, para cada $t$ em $T$ temos $(tE)^{f^{H/E}} = (Et)^{f^{H/E}} = E^f t^f = E^f s = sE^f$ logo $(T/E)^{f^{H/E}} = S/E^f$. ■

## 5.2 S-anéis e Digrafos de Cayley

Sejam $H$ um grupo finito e $S \subseteq H$ um subconjunto qualquer de $H$. Considere o digrafo $\mathrm{Cay}(H, S)$ de $H$ sobre $S$. Podemos considerar o S-anel $\langle\langle \widehat{S} \rangle\rangle$. Na verdade existe uma relação muito forte entre as propriedades de $\mathrm{Cay}(H, S)$ e de $\langle\langle \widehat{S} \rangle\rangle$. Para maiores detalhes precisamos da seguinte

**Definição 5.2.1.** *Seja $\mathcal{A} = \langle T_0, \ldots, T_d \rangle$ um S-anel sobre um grupo $H$. Definimos o* **grupo dos automorfismos de** $\mathcal{A}$ *como sendo*

$$\mathrm{Aut}(\mathcal{A}) = \bigcap_{i=0}^{d} \mathrm{Aut}(\mathrm{Cay}(H, T_i))$$

*isto é,* $\mathrm{Aut}(\mathcal{A})$ *consiste de todas as permutações* $\pi \in \mathrm{Sym}(H)$ *tais que:*
$h_1 h_2^{-1} \in T_i \Rightarrow h_1^{\pi}(h_2^{\pi})^{-1} \in T_i$, *para todo* $h_1, h_2 \in H$ *e para todo índice* $i$, $0 \leqslant i \leqslant d$.

**Proposição 5.2.2.** *Seja $H$ um grupo finito e $S \subseteq H$. Então:*

*i)* $\mathrm{Aut}(\langle\langle \widehat{S} \rangle\rangle) \leqslant \mathrm{Aut}(\mathrm{Cay}(H, S))$;

*ii) Se $\mathcal{B}, \mathcal{A}$ são dois S-anéis sobre o grupo $H$ com $\mathcal{B} \subseteq \mathcal{A}$ então* $\mathrm{Aut}(\mathcal{A}) \leqslant \mathrm{Aut}(\mathcal{B})$;

*iii) Dados $G$, $F$ em* $\mathrm{Sup}(R_H)$ *com $G \leqslant F$ então* $V(H, F_1) \subseteq V(H, G_1)$.

**Demonstração.** *i)* Como $\widehat{S} \in \langle\langle \widehat{S} \rangle\rangle$, a Proposição 3.2.2 garante que $S$ é uma união de conjuntos básicos de $\langle\langle \widehat{S} \rangle\rangle$. Sejam $f \in \mathrm{Aut}(\langle\langle \widehat{S} \rangle\rangle)$ e $\mathrm{Bsets}(\langle\langle \widehat{S} \rangle\rangle) = \{S_0, \ldots, S_t\}$. Assim $x \in \mathrm{Cay}(H, S) \Leftrightarrow x \in \mathrm{Cay}(H, S_j) = \mathrm{Cay}(H, S_j)^f \Leftrightarrow x \in \mathrm{Cay}(H, S)^f$.

*ii)* Sejam $\mathcal{B}, \mathcal{A}$ dois S-anéis sobre $H$ com $\mathcal{B} \subseteq \mathcal{A}$ e $\mathrm{Bsets}(\mathcal{A}) = \{T_0, \ldots, T_d\}$. Como $\mathcal{B} \subseteq \mathcal{A}$, para cada conjunto básico $S$ de $\mathcal{B}$ temos $\widehat{S} \in \mathcal{A}$. Isto nos diz que $S$ é um $\mathcal{A}$-subconjunto e, pela Proposição 3.2.2, $S$ é uma união de conjuntos básicos de $\mathcal{A}$. Com isso, se $f \in \mathrm{Aut}(\mathcal{A})$ então $\mathrm{Cay}(H, T_i)^f = \mathrm{Cay}(H, T_i)$ para todo índice $i$, $0 \leqslant i \leqslant d$. Em particular, $\mathrm{Cay}(H, T_i)^f = \mathrm{Cay}(H, T_i)$, para todo $T_i \in \mathrm{Bsets}(\mathcal{B})$ o que nos mostra que $f \in \mathrm{Aut}(\mathcal{B})$.

*iii)* Dados $G, F$ em $\mathrm{Sup}(R_H)$ e seja $x \in V(H, F_1)$. Como $G \leqslant F$ então $G_1 \leqslant F_1$ portanto $x^g = x$ para todo $g \in G_1$ e, pelo Lema 3.4.5, $x \in V(H, G_1)$. ■

**Proposição 5.2.3.** *Seja $\mathcal{A}$ um S-anel sobre um grupo $H$. Se $\mathcal{A} = V(H, G_1)$ para algum grupo $G$ em* $\mathrm{Sup}(R_H)$*, então $G \leqslant \mathrm{Aut}(\mathcal{A})$.*

**Demonstração.** Sejam $G \in \mathrm{Sup}(R_H)$ tal que $\mathcal{A} = V(H, G_1)$ e $T \in \mathrm{Bsets}(\mathcal{A})$. Dados $h_1, h_2$ dois elementos quaisquer de $H$, se $h_1 h_2^{-1} \in T$ então $h_1 \in Th_2$, ou seja, existe $\tilde{t}$ em $T$ tal que $h_1 = \tilde{t}h_2$. Agora, para todo $g$ em $G$ temos: $(\widehat{T}h_2)^g = [(\sum_{t\in T} t)h_2]^g = (\sum_{t\in T} th_2)^g = \sum_{t\in T}(th_2)^g$. Como $\widehat{T} \in \mathcal{A}$, pelo Lema 3.4.8, $(\widehat{T}h_2)^g = \widehat{T}h_2^g$ portanto $\sum_{t\in T}(th_2)^g = \sum_{t\in T} th_2^g$, isto é, existe $t \in T$ com $h_1^g = th_2^g$ implicando que $h_1^g(h_2^g)^{-1} \in T$, para todo $g \in G$.

Logo $G \leqslant \mathrm{Aut}(\mathcal{A})$. ■

Agora, estamos em condições de formular o resultado que relaciona $\mathrm{Cay}(H, S)$ e $\langle\langle \widehat{S} \rangle\rangle$.

**Teorema 5.2.4.** *Seja $H$ um grupo finito. Para cada $S \subseteq H$ temos*

$$\mathrm{Aut}(\mathrm{Cay}(H,S)) = \mathrm{Aut}(\langle\langle \widehat{S} \rangle\rangle).$$

**Demonstração.** Seja $G = \mathrm{Aut}(\mathrm{Cay}(H, S))$ e denote por $T_0, \ldots, T_s$ as órbitas de $G_1$. Dado $g$ em $G_1$, considere $y$ em $S^g$, isto é, um elemento da forma $y = x^g$ com $x \in S$. Mas $(y, 1) = (x^g, 1^g) \in \mathrm{Cay}(H, S)^g = \mathrm{Cay}(H, S)$,ou seja, $y = x^g \in S$. Usando este mesmo raciocínio, mostramos que $S \subseteq S^g$. Assim, $S = S^g$ implicando que $(\widehat{S})^g = \widehat{S}$ para todo $g \in G_1$ logo, pelo Lema 3.4.5, $\widehat{S} \in V(H, G_1)$. Mostramos que $V(H, G_1)$ é um S-anel que contém $\widehat{S}$; com isso podemos afirmar que $\langle\langle \widehat{S} \rangle\rangle \subseteq V(H, G_1)$. Por fim, aplicando as Proposições 5.2.2 e 5.2.3 temos

$$G = \mathrm{Aut}(\mathrm{Cay}(H, S)) \geqslant \mathrm{Aut}(\langle\langle \widehat{S} \rangle\rangle) \geqslant \mathrm{Aut}(V(H, G_1)) \geqslant G.$$

Aplicando o Teorema 5.2.4 no Exemplo 3.2.4 temos $\mathrm{Aut}(\mathrm{Cay}(C_8, \{g, g^7, g^4\})) = \mathrm{Aut}(\langle\langle \widehat{S} \rangle\rangle) \cong D_8$, onde $S = \{g, g^7, g^4\}$ e $D_8$ é o grupo diedral de ordem 16.

**Lema 5.2.5.** *Um S-anel $\mathcal{A}$ sobre um grupo $H$ é Schuriano se e somente se cada conjunto básico de $\mathcal{A}$ é uma órbita do grupo $G$ =Aut$(\mathcal{A})_1$.*

**Demonstração.** ($\Rightarrow$) Se $\mathcal{A}$ é Schuriano, existe $K \in \mathrm{Sup}(R_H)$ tal que $\mathcal{A} = V(H, K_1)$. Pela Proposição 5.2.3, temos que $K \leqslant \mathrm{Aut}(\mathcal{A})$ logo; pela Proposição 5.2.2, $V(H,G) \leqslant V(H,K_1) = \mathcal{A}$. Mas dado $x \in \mathcal{A}$, existem $\alpha_1, \ldots, \alpha_s$ em $\mathbb{Q}$ tais que $x = \sum_{k=0}^{s} \alpha_k \widehat{T_k}$. Portanto $x^g = \sum_{k=0}^{s} \alpha_k (\widehat{T_k})^g = \sum_{k=0}^{s} \alpha_k \widehat{T_k} = x$, para todo $g \in G$ pois $T_k^g = T_k$. Pelo Lema 3.4.5 , $x \in V(H,G)$ logo $\mathcal{A} = V(H,G)$ o que nos mostra que todo conjunto básico de $\mathcal{A}$ é uma órbita de $G$.

($\Leftarrow$) Suponhamos que cada conjunto básico de $\mathcal{A}$ é uma órbita de $G$ =Aut$(\mathcal{A})_1$. Pela Proposição 2.1.12, Aut$(\mathcal{A}) \in \mathrm{Sup}(R_H)$. Portanto, $\mathcal{A}$ é Schuriano. ■

**Proposição 5.2.6.** *Seja $\mathcal{A}$ um S-anel Schuriano (Definição 3.4.10) sobre o grupo $H$. Então para um $\mathcal{A}$-subgrupo arbitrário $E \leqslant H$ as seguintes propriedades são verdadeiras:*

*(i) $\mathcal{A}_E$ é Schuriano; e*

*(ii) Se $E$ é normal em $H$, então $\mathcal{A}/E$ é Schuriano.*

**Demonstração.** *(i)* Sejam $f \in G$ =Aut$(\mathcal{A})_1$ e $T$ em Bsets$(\mathcal{A})$.

*Afirmação:* $T^f = T$

Seja $x \in T$. Então o par $(x, 1)$ pertence ao conjunto Cay$(H,T)$=Cay$(H,T)^f$, isto é, existe $y$ em $T$ com $(x,1) = (y^f, 1^f)$ logo $x = y^f \in T^f$. Por outro lado, se $y \in T^f$ existe $x \in T$ tal que $y = x^f$. Além disso, $(y,1) = (x^f, 1^f) \in \mathrm{Cay}(H,T)^f = \mathrm{Cay}(H,T)$. Portanto $y \in T$ o que prova a afirmação .

Com isso, $xy^{-1} \in T \Leftrightarrow x^f(y^f)^{-1} \in T$ mostrando que $f$ é um automorfismo combinatório normalizado de $\mathcal{A}$. Pela Proposição 5.1.9, $f_E$ é um isomorfismo combinatório normalizado entre $\mathcal{A}_E$ e $\mathcal{A}_{E^f}^f$. Mas $E$ é um $\mathcal{A}$-subgrupo, ou seja, existem conjuntos básicos de $\mathcal{A}$, $T_{i_1}, \ldots, T_{i_s}$ tais que $E = \bigcup_{j=0}^{s} T_{i_j}$ logo $E^f = (\bigcup_{j=0}^{s} T_{i_j})^f = \bigcup_{j=0}^{s} (T_{i_j})^f = \bigcup_{j=0}^{s} T_{i_j} = E$. Como $\mathcal{A}^f = \mathcal{A}$ então $f_E$ é um automorfismo combinatório de $\mathcal{A}_E$.

Considere o conjunto $G_E = \{f_E \mid f \in G\}$. Dado $T$ em $\mathrm{Bsets}(\mathcal{A}_E)$ então $T$ pertence a $\mathrm{Bsets}(\mathcal{A})$ e $T \subseteq E$ logo $G_E \leqslant \mathrm{Aut}(\mathcal{A}_E)$. Além disso, $T$ é uma órbita de $G$ mas $G$ e $G_E$ possuem as mesmas órbitas em $E$ portanto $T$ é uma órbita do grupo $\mathrm{Aut}(\mathcal{A}_E)_1$ e pelo Lema 5.2.5, $\mathcal{A}_E$ é Schuriano.

*(ii)* Seja $f \in G = \mathrm{Aut}(\mathcal{A})_1$. Na demonstração do item anterior vimos que $f$ é um automorfismo combinatório normalizado de $\mathcal{A}$.

*Afirmação:* $\big(H/E\big)^f = H/E$

Seja $Eh$ um elemento de $H/E$. Existe $h_1$ em $H$ tal que $h = h_1^f$. Como $E^f = E$, temos $Eh = E^f h_1^f = (Eh_1)^f$ logo $Eh \in \big(H/E\big)^f$. Mas $(Eh)^f = E^f h^f = Eh^f \in H/E$ mostrando que $\big(H/E\big)^f = H/E$ o que prova a afirmação .

Assim pela parte *(iii)* da Proposição 5.1.9, temos que $f^{H/E}\colon H/E \longrightarrow H/E$ é um automorfismo combinatório normalizado de $\mathcal{A}/E$. Considere o conjunto $G^{H/E} = \{f^{H/E} \mid f \in G\}$. Como $(tE)^{f^{H/E}} = (Et)^{f^{H/E}} = E^f t^f = t^f E$, obtemos que $(tE)^{G^{H/E}} = \{t^g E \mid g \in G\} = t^G/E = T/E$. Assim, $T/E$ é uma órbita de $G^{H/E}$ e portanto uma órbita de $\mathrm{Aut}(\mathcal{A}/E)_1$. O resultado segue do Lema 5.2.5. ■

## Configurações Coerentes Homogêneas

Uma *configuração* $\mathcal{C} = (X, (f_i)_{i\in I})$ *em* $X$ *sobre um conjunto* $I$ consiste de um conjunto finito não vazio $X$ juntamente com uma família $(f_i)_{i\in I}$ não vazia de relações binárias em $X$. Dada uma configuração $\mathcal{C} = (X, (f_i)_{i\in I})$ em $X$ escrevemos:

$$f_i(x) = \{y \in X \mid (x,y) \in f_i\} \;\; x \in X;$$
$$f_i^t = \{(y,x) \mid (x,y) \in f_i\};$$
$$\Delta = \{(x,x) \mid x \in X\}.$$

**Definição 5.2.7.** *Uma configuração* $\mathcal{C} = (X, (f_i)_{i\in I})$ *em* $X$ *sobre um conjunto* $I$ *diz-se uma* **configuração coerente homogênea** *se satisfaz as seguintes propriedades:*

1. $(f_i)_{i\in I}$ *é uma partição de* $X^2$,

2. $f_i^t = f_{i'}, i' \in I$,

3. *existe* $i \in I$ *tal que* $f_i = \Delta$

4. *para toda tripla* $i, j, k$ *em* $I$, *o número* $|f_i(x) \cap f_j^t(y)|$ *independe da escolha de* $(x, y)$ *em* $f_k$

**Definição 5.2.8** (Isomorfismos entre Configurações Coerentes). *Sejam* $(\Omega, S_i)_{i\in I}$ *e* $(\Omega', S'_j)_{j\in J}$ *duas configurações coerentes. Um* **isomorfismo de** $(\Omega, S_i)$ *em* $(\Omega', S'_j)$ *é uma aplicação bijetora* $\phi\colon \Omega \cup S_i \longrightarrow \Omega' \cup S'_j$ *tal que* $\Omega' = \Omega^\phi, S'_j = S_i^\phi$ *e* $(ws)^\phi = w^\phi s^\phi$ *para todo* $s$ *em* $S_i$ *e* $w$ *em* $D(s) = \{w \in \Omega \mid ws \neq \emptyset\}$ *e* $ws = \{\alpha \in \Omega \mid (w, \alpha) \in s\}$.

O principal objetivo desta seção é relacionar os conceitos de isomorfismos entre configurações coerentes e isomorfismos entre S-anéis. Para tanto, precisamos do seguinte

**Teorema 5.2.9.** *Seja* $\mathcal{A}$ *um S-anel sobre um grupo finito* $H$ *e* $\mathrm{Bsets}(\mathcal{A}) = \{T_0, \ldots, T_d\}$. *Para cada* $T_i$ *em* $\mathrm{Bsets}(\mathcal{A})$ *considere a relação binária* $\mathrm{Cay}(H,T_i) = \{(x, y) \mid xy^{-1} \in T_i\}$. *Então:*

1. $\{\mathrm{Cay}(H, T_i)\}_{i=0}^d$ *particiona* $H \times H$;

2. $\Delta_H = \mathrm{Cay}(H, T_0)$;

3. *Para cada* $T_i$ *em* $\mathrm{Bsets}(\mathcal{A})$ *temos* $\mathrm{Cay}(H, T_i)^t = \mathrm{Cay}(H, T_i^{(-1)})$;

4. *Para toda tripla* $i, k, j$ *de elementos em* $\{0, \ldots, d\}$ *o número* $\theta_t(\widehat{T_i}, \widehat{T_j})$ *é constante para todo* $t$ *em* $T_k$.

**Demonstração.**

1. Seja $(x, y)$ um elemento qualquer de $H \times H$. Como $H$ é um grupo, o elemento $xy^{-1}$ pertence a $H$ logo existe $i, 0 \leqslant i \leqslant d$, tal que $xy^{-1} \in T_i$ uma vez que $\cup T_i = H$. Isto implica que $(x, y) \in \mathrm{Cay}(H, T_i)$. Agora, se $i \neq j$, temos que $\mathrm{Cay}(H, T_i) \cap \mathrm{Cay}(H, T_j) = \emptyset$ pois $T_i \cap T_j = \emptyset$. Portanto $\bigcup_{i=0}^{d} \mathrm{Cay}(H, T_i) = H \times H$ e $\mathrm{Cay}(H, T_i) \cap \mathrm{Cay}(H, T_j) = \emptyset$.

*2.* A demonstração é imediata.

*3.* Seja $T_i$ em Bsets($\mathcal{A}$) e considere Cay$(H, T_i)$. Como $\mathcal{A}$ é um S-anel, existe $j$, $0 \leqslant j \leqslant d$, tal que $T_j = T_i^{(-1)}$. Assim $(x, y) \in \text{Cay}(H, T_j) \Leftrightarrow xy^{-1} \in T_j \Leftrightarrow (xy^{-1})^{-1} = yx^{-1} \in T_i \Leftrightarrow (y, x) \in \text{Cay}(H, T_i)$. Logo Cay$(H, T_i)^t$=Cay$(H, T_j)$.

*4.* A demonstração é consequência direta da Proposição 3.1.6. ■

Em outras palavras, mostramos que $\mathcal{C} = (H, \{\text{Cay}(H, T_i)\}_{i=0}^d)$ é uma configuração coerente homogênea em $H$.

Sejam $\mathcal{A}$ e $\mathcal{B}$ dois S-anéis sobre os grupos finitos $H$ e $K$ respectivamente. Sejam ainda Bsets($\mathcal{A}$) $= \{T_0, \ldots, T_d\}$ e Bsets($\mathcal{B}$) $= \{S_0, \ldots, S_t\}$. Se $f\colon H \longrightarrow K$ é uma bijeção tal que $\left(\{\text{Cay}(H, T_i)\}_{i=0}^d\right)^f = \{\text{Cay}(K, S_j)\}_{j=0}^t$ então para todo $w \in D(\text{Cay}(H, T_i))$ tem-se que $(w\text{Cay}(H, T_i))^f = w^f \text{Cay}(H, T_i)^f$. Por outro lado, pelo Teorema 5.2.9, sabemos que $(H, \{\text{Cay}(H, T_i)\}_{i=0}^d)$ e $(K, \{\text{Cay}(K, S_j)\}_{j=0}^t)$ formam duas configurações coerentes homogêneas em $H$ e $K$ respectivamente.

Suponhamos que tais configurações sejam isomorfas; então existe uma aplicação

$$f\colon H \cup \{\text{Cay}(H, T_i)\}_{i=0}^d \longrightarrow K \cup \{\text{Cay}(K, S_j)\}_{j=0}^t$$

bijetora tal que

1. $H^f = K$;
2. $\left(\{\text{Cay}(H, T_i)\}_{i=0}^d\right)^f = \{\text{Cay}(K, S_j)\}_{j=0}^t$ e
3. $(w\text{Cay}(H, T_i))^f = w^f \text{Cay}(H, T_i)^f$, para todo $w \in D(\text{Cay}(H, T_i))$.

Podemos concluir que as configurações coerentes homogêneas $(H, \{\text{Cay}(H, T_i)\}_{i=0}^d)$ e $(K, \{\text{Cay}(K, S_j)\}_{j=0}^t)$ são isomorfas se e somente se existe uma função bijetora $f\colon H \longrightarrow K$ tal que para cada $T_i$ em Bsets($\mathcal{A}$) existe $S_j$ em Bsets($\mathcal{B}$) tal que Cay$(H, T_i)^f$ =Cay$(K, S_j)$ ou, equivalentemente, se $f$ é um isomorfismo combinatório entre $\mathcal{A}$ e $\mathcal{B}$. Portanto isomorfismos combinatórios entre S-anéis são isomorfismos entre configurações coerentes homogêneas.

# Referências Bibliográficas


[1] B. Alspach, T. D. Parsons, *Isomorphism of circulant graphs and digraphs*, Discrete Math. 25 (1979) 97-108.

[2] D. Gluck , *A note on permutation polynomials and finite geometry* , Discrete Math. 80 (1990) 97-100.

[3] C. Godsil, G. Royle, *Algebraic Graph Theory*, Springer, 2001.

[4] D.G. Higman, *Coherent Algebras*, Linear Algebra Appl. 93 (1987) 209-239.

[5] Y. Hiramine , *A conjucture on affine planes of prime order*, J. Combin. Theory Ser. A 52 (1989) 44-50.

[6] M. Hirasaka, M. Muzychuk, *An elementary Abelian group of rank 4 is a CI-group*, J. Combin. Theory Ser. A 94 (2) (2001) 339-362.

[7] M. Muzychuk, *An elementary Abelian group of large rank is not a CI-group*, Discrete Math. 264 (1-3) (2003) 167-185.

[8] M. Muzychuk, *On the Structure of Basic Sets of Schur Rings over Cyclic Groups*, Journal of Algebra 169 (1994) 655-678.

[9] C. Polcino Milies, S.K. Sehgal, *An Introduction to Group Rings*, Kluwer Academic Publishers, Dordrecht, Boston, London, 2001.

[10] L. Rónyai, T. Szönyi , *Planar functions over finite fields* , Combinatorica 9 (3) (1989) 315-320.

[11] W.R. Scott, *Group Theory*, Dover Publications, Inc., New York, 1964.

[12] P. Spiga, Q. Wang, *An answer to Hirasaka and Muzychuk: Every p-Schur ring over $C_p^3$ is Schurian*, Discrete Mathematics (308) (2008) 1760-1763.

[13] H. Wielandt, *Finite Permutation Groups*, Academic Press, Berlin, 1964.

[14] P.H. Zieschang, *An algebraic approach to association schems* in Lecture Notes in Mathematics, vol. 1628, Springer, New York, Berlin, 1996.