UNIVERSIDADE ESTADUAL DO SUDOESTE DA BAHIA
Departamento de Ciências Exatas e Tecnológicas

GISLAINE DUARTE DE SOUZA

UM ESTUDO DAS ESTRUTURAS QUOCIENTES:
dos Grupos às Álgebras com Identidades Polinomiais

Vitória da Conquista - Bahia
2021

GISLAINE DUARTE DE SOUZA

UM ESTUDO DAS ESTRUTURAS QUOCIENTES:
dos Grupos às Álgebras com Identidades Polinomiais

Monografia apresentada ao Departamento de Ciências Exatas e Tecnológicas da Universidade Estadual do Sudoeste da Bahia - Campus Vitória da Conquista-BA, para obtenção do Título de Licenciado em Matemática, sob orientação do Prof. Dr. Júlio César dos Reis.

Vitória da Conquista - Bahia
2021

Folha de aprovação

Gislaine Duarte de Souza

Um Estudo das Estruturas Quocientes:
dos Grupos às Álgebras com Identidades Polinomiais

Monografia apresentada ao Colegiado do Curso de Matemática como requisito parcial para aprovação na disciplina Seminário de Pesquisa II do Curso de Licenciatura em Matemática.

Aprovado em: 04 de junho de 2021.

BANCA EXAMINADORA

Prof. Dr. Júlio César dos Reis - UESB
Orientador

Prof. Dr. Fernanda Gonçalves de Paula
UESC

Prof. Dr. Flaulles Boone Bergamaschi
UESB

Vitória da Conquista - BA
2021

Aos meus amados pais, Arnaldo e Vilma, e
minha irmãzinha, Lorrany Victória.

Agradecimentos

Agradeço primeiramente à Deus, por sempre me amparar, me dar forças para continuar e se mostrar presente em todos os momentos da minha vida. Sem ele não seria nada!

Agradeço aos meus pais, Arnaldo Dias de Souza e Vilma de Jesus Duarte Souza, pois, se cheguei até aqui foi graças à eles, que não mediram esforços para que eu pudesse estudar. Muito obrigada, amo vocês!

Agradeço também à minha irmãzinha, Lorrany Victória, que mesmo sem saber me inspira e me dá forças para seguir em frente. Sua alegria é contagiante. Te amo pequena!

Não poderia deixar de agradecer ao professor Júlio César dos Reis por toda a orientação durante esse processo. O senhor foi fundamental para que isso se tornasse possível, sempre paciente, me aconselhando e incentivando. O senhor foi um orientador maravilhoso, muito obrigada!

Agradeço também as irmãzinhas que a vida me deu, Betânia e Flávia, por todo esse tempo que passamos juntas, nos ajudando, rindo, chorando e aconselhando. Muito obrigada, meninas!

Agradeço aos amigos que a UESB me deu, Débora, Mateus e Samuel, pelos dias de estudo suados nos quais nos desesperamos, choramos, mas acima de tudo, rimos muito e nos ajudamos. Vocês são incríveis! Agradeço também ao meu amigo Bruno, por sempre ter me ajudado nos estudos, principalmente quando se tratava de álgebra. Comecei a gostar da área graças à você!

Quero agradecer aos meus demais familiares que sempre me incentivaram e acreditaram em mim. Em especial, agradeço ao meu avô, Antônio José Duarte (*in memorian*), que ficou tão feliz quando soube que eu entraria na universidade que saiu falando pra todo mundo com um sorrisão de orelha à orelha, todo orgulhoso. Uma pena o senhor não estar mais aqui para me ver formada. Sinto sua falta!

RESUMO

Este trabalho tem como objetivo central fazer um estudo detalhado da construção do quociente nos grupos, anéis, espaços vetoriais e álgebras. Dividido em seis capítulos, sendo quatro deles destinados especificamente a construção do quociente em cada uma dessas estruturas, trazemos definições, exemplos, proposições e teoremas que são importantes para entender o que vem a ser o quociente.

Ao longo da construção do quociente percebe-se semelhanças e diferenças existentes entre as estruturas. Veremos que para se chegar ao quociente em cada uma delas é seguido um padrão: equivalência, classes laterais, subconjuntos, conjunto de classes laterais e operações bem definidas que obedecem a certas propriedades.

Sumário

Introdução

No presente trabalho fazemos um estudo sobre a estrutura quociente de diferentes estruturas algébricas, utilizando de diferentes bibliografias que abordam o tema, buscamos observar as diferenças e semelhanças entre os quocientes dessas estruturas. Dessa forma, começando com grupos, passando por anéis e espaços quocientes, e enfim chegando às álgebras com identidades polinomiais, mostramos que apesar de se tratar de estruturas diferentes, com propriedades e comportamentos diferentes, a construção do quociente em cada uma delas se dá de forma bastante semelhante.

O trabalho está dividido em seis capítulos. Cada capítulo traz definições, teoremas, algumas demonstrações relevantes e exemplos, afinal, nada melhor do que exemplificar o que está sendo estudado.

No capítulo 1, trazemos apenas as definições de grupo, anéis e espaços vetoriais. Trata-se de um capítulo de revisão, ou melhor, um capítulo base, uma vez que essas definições serão importantes ao longo do trabalho.

No Capítulo 2 falamos sobre a construção do grupo quociente. Em linhas gerais, tomamos um subgrupo H normal a um grupo G. O conjunto das classes laterais à esquerda de H com relação a G e é denotado por

$$G/H = \{xH;\ x \in G\}.$$

Ao definir uma operação nesse conjunto e verificar que a mesma está bem definida, ou seja, que não depende da escolha dos representantes, não é difícil mostrar que esse conjunto é também um grupo, chamado de grupo quociente.

No Capítulo 3 estudamos os anéis quocientes. Na construção dos anéis quocientes utilizamos ideais I no anel A. Definida a classe lateral de I em relação à A, o conjunto dessas classes laterais é denotado por

$$A/I = \{a + I;\ a \in A\}.$$

Uma vez definidas as operações de adição e multiplicação nesse conjunto e verificada que elas estão bem definidas, não é difícil mostrar que esse conjunto é também um anel, o anel quociente.

No Capítulo 4 falamos sobre os espaços quocientes. O processo de construção dessa estrutura é semelhante ao de grupos e anéis quocientes. Para essa construção é indispensável

tomarmos um espaço vetorial V sobre um corpo $\mathbb{F}$ e um subespaço W de V. Definida a congruência de vetores de V módulo W, essa congruência é uma relação de equivalência sobre V. As classes de equivalência dessa relação são conhecidas como as classes laterais de W e o conjunto de todas as classes laterais é denotado por

$$V/W = \{\alpha + W;\ \alpha \in V\}.$$

Ao definir as operações de adição de vetores e multiplicação por escalar nesse conjunto e mostrando que ambas estão bem definidas, é fácil verificar que o mesmo é também um espaço vetorial, chamado de espaço quociente.

Por fim, no Capítulo 5 estudamos as álgebras quocientes. Para isso, vimos a definição de álgebra e alguns exemplos, para enfim apresentar um exemplo concreto de uma álgebra quociente que desempenha papel fundamental na PI-teoria. Desse modo, nos aprofundamos um pouco mais na teoria de álgebras e estudamos as álgebras com identidades polinomiais, T-ideais e álgebras com identidades polinomiais graduadas.

Capítulo 1

Algumas definições importantes

Nesse capítulo traremos a definição de grupos, anéis e espaços vetoriais, bem como alguns exemplos de cada uma dessas estruturas. Não poderíamos falar do quociente de estruturas algébricas sem antes recordar essas definições vistas durante a graduação e que serão tão importantes para entendermos o tema de cada um dos capítulos seguintes. Entender o que são anéis e espaços vetoriais, por exemplo, é essencial para entender uma estrutura algébrica muito interessante cujo quociente será trabalhado no Capítulo 5,a saber, as álgebras.

Neste capítulo não demonstraremos nenhum dos exemplos de grupos, anéis, ou espaços vetoriais, uma vez que este não é o propósito do trabalho.

1.1 Definição de Grupos

Definição 1.1.1 *Sejam G um conjunto não vazio e $*$ uma operação binária. Dizemos que G, munido dessa operação, é um grupo se as seguintes condições são satisfeitas.*

1. $\forall\ a, b, c \in G,\ a * (b * c) = (a * b) * c$ *(Associatividade);*
2. $\forall\ a \in G,\ \exists\ e \in G,\ tal\ que\ a * e = e * a = a$ *(Elemento neutro);*
3. $\forall\ a \in G,\ \exists\ b \in G,\ tal\ que\ a * b = b * a$ *(Elemento simétrico).*

Definição 1.1.2 *Um grupo G é chamado de* **grupo abeliano** *, ou grupo comutativo se a operação $*$ é comutativa, ou seja, para quaisquer $a,\ b \in G$, vale:*

$$a * b = b * a.$$

Vejamos a seguir alguns exemplos de grupos e também de grupos abelianos, apenas para relembrar algumas definições importantes para que possamos entender o que estudaremos mais adiante. São exemplos de grupos abelianos:

Exemplo 1.1.3 *O conjunto dos números inteiros $\mathbb{Z}$, munido da operação de usual de adição.*

Exemplo 1.1.4 *O conjunto dos números racionais $\mathbb{Q}$, munido da operação de adição.*

Exemplo 1.1.5 *O conjunto dos números reais $\mathbb{R}$, munido da operação de adição.*

Exemplo 1.1.6 *O conjunto $\mathbb{Q} - \{0\}$, munido da operação usual de multiplicação.*

Exemplo 1.1.7 *O conjunto $\mathbb{R} - \{0\}$, com a operação usual de multiplicação.*

Exemplo 1.1.8 *O conjunto $\mathbb{C} - \{0\}$, com a operção usual de multiplicação.*

Exemplo 1.1.9 *O conjunto dos números complexos $\mathbb{C}$, munido da operação de adição.*

Observação 1.1.10 *Note que os conjuntos $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$, munidos da operação usual de multiplicação, não são grupos, pois o 0 não possui inverso em nenhum destes conjuntos.*

Exemplo 1.1.11 *O conjunto de classes residuais módulo n, denotado por $\mathbb{Z}_n$, com a operação de adição dada por:*

$$\overline{a} + \overline{b} = \overline{a + b}$$

é um grupo abelino.

Exemplo 1.1.12 *O conjunto formado pelos elementos inverstíveis de $\mathbb{Z}_n$, denotado por $\mathbb{U}_n$, com a operação:*

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

é um grupo abeliano.

Veremos mais alguns exemplos de grupos no próximo capítulo.

1.2 Definição de Anéis

Definição 1.2.1 *Seja A um conjunto não vazio munido de duas operações binárias, adição $(+)$ e multiplicação $(\cdot)$. Dizemos que$(A, +, \cdot)$ é um anel se obedece as seguintes condições:*

Sejam a, b e $c \in A$

1. $a + b = b + a$ *(Comutatividade);*
2. $(a + b) + c = a + (b + c)$ *(Associatividade);*
3. $\exists\ 0 \in A,\ tal\ que,\ a + 0 = 0 + a = a$ *(Elemento Neutro);*
4. $\exists - a \in A,\ tal\ que, a + (-a) = a - a = 0$ *(Simétrico Aditivo);*
5. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *(Associatividade);*
6. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ *(Distributividade);*
7. $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ *(Distributividade).*

Vemos que os itens de 1 à 4, que chamamos de axiomas, apenas afirmam que A é um grupo abeliano com relação a adição. Já os axiomas 6 e 7 afirmam que A é fechado e associativo em relação à mutiplicação, ou seja, A é um anel associativo.

Além disso, quando o anel A possui elemento neutro na multiplicação, ou seja, $\forall\ a \in A,\ \exists\ 1 \in A,\ tal\ que\ a \cdot 1 = 1 \cdot a = a$, o chamamos de anel com unidade. Já quando o anel A satisfaz a comutatividade do produto, ou seja, $\forall\ a, b \in A,\ temos\ que\ a \cdot b = b \cdot a$, o chamamos de anel comutativo. Vejamos a seguir alguns exemplos de anéis.

Exemplo 1.2.2 *O conjunto dos números reais $\mathbb{R}$ é um anel.*

Exemplo 1.2.3 *O conjunto dos números complexos $\mathbb{C}$ é um anel.*

Exemplo 1.2.4 *O conjunto das matrizes $M_n(F)$ com $F = \mathbb{Z},\ \mathbb{Q},\ \mathbb{R}, ou\ \mathbb{C}$ é um anel.*

Observação 1.2.5 *Mais exemplos de anéis serão encontrados no Capítulo 3, a partir da página 22.*

Definição 1.2.6 *Dizemos que um anel com unidade $\mathbb{K}$ é um corpo se, $\forall\ a, b \in \mathbb{K}$, as seguintes condições são satisfeitas:*

1. $a \cdot b = b \cdot a$

2. Para cada $a \in \mathbb{K}$ existe a', tal que $a \cdot a' = a' \cdot a = 1$.

Em outras palavras, um corpo $\mathbb{K}$ é um anel comutativo com unidade, tal que todos os seus elementos admitem simétrico multiplicativo.

Vejamos abaixo alguns exemplos de corpos.

Exemplo 1.2.7 *O conjunto dos números racionais $\mathbb{Q}$ com as operações usuais de adição e multiplicação é um corpo.*

Exemplo 1.2.8 *O conjunto dos números reais $\mathbb{R}$ é um corpo.*

Exemplo 1.2.9 *O conjunto $\mathbb{Z}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ é um corpo, pois, é comutativo com relação a multiplicação, e cada elemento não nulo desse conjunto possui simétrico multiplicativo como podemos ver abaixo:*

- $\bar{1} \cdot \bar{1} = \bar{1} = \bar{6} \cdot \bar{6}$
- $\bar{2} \cdot \bar{4} = \bar{1} = \bar{4} \cdot \bar{2}$
- $\bar{3} \cdot \bar{5} = \bar{1} = \bar{5} \cdot \bar{3}$

Exemplo 1.2.10 *Do mesmo modo, os anéis $\mathbb{Z}_2$ e $\mathbb{Z}_3$ são corpos.*

Exemplo 1.2.11 *O anel dos complexos $\mathbb{C}$ é também um corpo.*

Definição 1.2.12 *Seja um corpo $\mathbb{K}$. Dizemos que a característica de $\mathbb{K}$ é igual a n, denotamos por $char\mathbb{K} = n$, se n é o menor inteiro positivo tal que*

$$\{\underbrace{1 + 1 + \cdots + 1}_{n \ \ vezes}\} = 0$$

Caso não exista esse n, dizemos que $char\mathbb{K} = 0$.

Exemplo 1.2.13 *Veja que nos corpos $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ não existe um n de forma que $\underbrace{1 + 1 + \cdots + 1}_{n \ \ vezes}$ seja igual a zero. Portanto, temos $char\ \mathbb{Q} = char\ \mathbb{R} = char\ \mathbb{C} = 0$.*

Exemplo 1.2.14 *A característica do conjunto $\mathbb{Z}_p$ é p.*

Observação 1.2.15 *A característica de um corpo é sempre 0 ou um número primo. Dessa forma, um corpo finito têm sempre um número primo como característica.*

Definição 1.2.16 *Um anel A é chamado* **domínio de integridade** *se:*

- *A é comutativio;*
- *A possui o elemento identidade 1;*
- *A não possui divisores de zero, ou seja, $ab \neq 0$ $\forall a, b \in A$ com $a \neq 0 \neq b$;*
- *$0 \neq 1$ pois, se $0 = 1$ então $a = a \cdot 1 = a \cdot 0 = 0$. Assim, se $0 = 1$, então $R = \{0\}$.*

Exemplo 1.2.17 *Os anéis $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ não têm divisores de zero e, portanto, são domínios de integridade. Note que nestes conjuntos se $ab = 0$, então $a = 0$ ou $b = 0$.*

Exemplo 1.2.18 *O anel $\mathbb{Z}_6$, por exemplo, não é um domínio de integridade, pois, $2 \cdot 3 = 0$, mas $2 \neq 0 \neq 3$. Portanto, 2 e 3 são divisores de 0.*

1.3 Definição de Espaços Vetoriais

Definição 1.3.1 *Seja V um conjunto não vazio munido de uma operação binária $+$ e uma operação mista $\cdot : \mathbb{K} \times V \to V$, esta última chamada de multiplicação por escalar. Dizemos que V é um espaço vetorial sobre o corpo $\mathbb{K}$ se for um grupo abeliano em relação a operação de adição de vetores e se, com relação à multipicação por escalar, as seguintes condições são satisfeitas:*

1. *$\alpha \cdot (v + w) = \alpha \cdot v + \alpha \cdot w$ (Distributividade);*
2. *$(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v$ (Distributividade);*
3. *$\alpha \cdot (\beta \cdot v) = (\alpha \cdot \beta) \cdot v$ (Associatividade);*
4. *$1 \cdot v = v$ (Elemento Neutro).*

para todo $\alpha, \beta \in \mathbb{K}$ e $v,\ w \in V$, onde 1 é a unidade de $\mathbb{K}$ com relação à multiplicação.

Em resumo, um espaço vetorial é uma estrutura algébrica composta por um corpo, um conjunto de vetores e duas operações que obedecem a certas propriedades. Vejamos a seguir alguns exemplos.

Exemplo 1.3.2 *O conjunto dos números reais $\mathbb{R}$ é um espaço vetorial.*

Exemplo 1.3.3 *O conjunto dos números complexos $\mathbb{C}$ é um espaço vetorial.*

Exemplo 1.3.4 *O conjunto das matrizes $M_{m\times n}(\mathbb{R})$ é um espaço vetorial sobre $\mathbb{R}$.*

Exemplo 1.3.5 *O conjunto de todas as n-uplas de números reais, denotado por* $\mathbb{R}^n$*, é um espaço vetorial. O* $\mathbb{R}^n$ *pode ser visto como um espaço vetorial sobre* $\mathbb{R}$ *desde que a adição e multiplicação sejam definidas da seguinte maneira: Sejam* $\alpha = (x_1,\ x_2, \cdots,\ x_n)$ *e* $\beta = (y_1,\ y_2, \cdots,\ y_n)$*, com* $x_i, y_i \in \mathbb{R}$

$$\alpha + \beta = (x_1,\ x_2,\ \cdots,\ x_n) + (y_1,\ y_2,\ \cdots,\ y_n) = (x_1 + y_1,\ x_2 + y_2,\ \cdots,\ x_n + y_n)$$
$$c\alpha = c(x_1,\ x_2,\ \cdots,\ x_n) = (cx_1,\ cx_2,\ \cdots,\ cx_n).$$

Observação 1.3.6 *Veremos mais exemplos de espaços vetoriais no Capítulo 4.*

Neste capítulo relembramos algumas definições que serão fundamentais para entendermos o conteúdo que será estudado nos próximos capítulos. É importante ressaltar que estas definições são estudadas durante a graduação, e portanto, nos são familiares. No capítulo 5, no entanto, traremos a definição de uma estrutura álgebrica que, ao contrário das demais, não é estudada durante a graduação, a saber, a estrutura de álgebra.

Capítulo 2

Grupos Quocientes

2.1 Classes Laterais

Nesta seção definiremos classes laterais e traremos algumas de suas propriedades básicas. Esse estudo será de extrema importância para mais à frente estudarmos o Teorema de Lagrange, subgrupos normais e Grupos Quocientes.

Definição 2.1.1 *Seja (G, *) um grupo e H um subgrupo de G. Para cada x, y ∈ G, podemos estabelecer a seguinte relação:*

$$y \tilde{e} x \Leftrightarrow \exists\ h \in H\ tal\ que\ y = xh.$$

Prova-se que esta relação, de fato, é de equivalência.
Chamamos de **classe lateral** *à esquerda de H em G que contém x o conjunto:*

$$x * H = \{x * h;\ h \in H\}.$$

Quando não houver confusão possível, chamaremos essa classe apenas de classe lateral de x à esquerda.

Analogamente, podemos definir a seguinte relação de equivalência:

$$y \tilde{d} x \Leftrightarrow \exists\ h \in H\ tal\ que\ y = hx.$$

Denominamos de classe lateral à direita de H em G que contém x o conjunto:

$$H * x = \{h * x;\ h \in H\}$$

que chamaremos de classe lateral de x à direita quando não houver confusão possível.

Observação 2.1.2 *Note que se G for um grupo comutativo $x * H = H * x$, ou seja, a classe lateral à esquerda de x é igual a classe lateral à direita de $x, \forall x \in G$.*

A seguir veremos alguns exemplos de classes laterais. Note que podemos construir classes laterais tanto de grupos aditivos quanto de grupos multiplicativos.

Exemplo 2.1.3 *Seja o grupo multiplicativo $G = \{1, i, -1, -i\}$ e $H = \{1, -1\}$ seu subgrupo. Temos as seguintes classes laterais:*

- $1 \cdot H = \{1 \cdot 1, 1 \cdot (-1)\} = \{1, -1\} = H \cdot 1$
- $(-1) \cdot H = \{(-1) \cdot 1, (-1) \cdot (-1)\} = \{-1, 1\} = H \cdot (-1)$
- $i \cdot H = \{i \cdot 1, i \cdot (-1)\} = \{i, -i\} = H \cdot i$
- $(-i) \cdot H = \{(-i) \cdot 1, (-i) \cdot (-1)\} = \{-i, i\} = H \cdot (-i)$

Exemplo 2.1.4 *Sejam o grupo aditivo $G = \mathbb{Z}_6$ e seu subgrupo $H = \{\overline{0}, \overline{3}\}$. Temos as seguintes classes laterais:*

- $\overline{0} + H = \{\overline{0} + \overline{0}, \overline{0} + \overline{3}\} = \{\overline{0}, \overline{3}\} = H + \overline{0}$
- $\overline{1} + H = \{\overline{1} + \overline{0}, \overline{1} + \overline{3}\} = \{\overline{1}, \overline{4}\} = H + \overline{1}$
- $\overline{2} + H = \{\overline{2} + \overline{0}, \overline{2} + \overline{3}\} = \{\overline{2}, \overline{5}\} = H + \overline{2}$
- $\overline{3} + H = \{\overline{3} + \overline{0}, \overline{3} + \overline{3}\} = \{\overline{3}, \overline{0}\} = H + \overline{3}$
- $\overline{4} + H = \{\overline{4} + \overline{0}, \overline{4} + \overline{3}\} = \{\overline{4}, \overline{1}\} = H + \overline{4}$
- $\overline{5} + H = \{\overline{5} + \overline{0}, \overline{5} + \overline{3}\} = \{\overline{5}, \overline{2}\} = H + \overline{5}$

Observação 2.1.5 *No exemplo acima podemos notar que, como o grupo $G = \mathbb{Z}_6$ é comutativo, as classes laterais à esquerda e à direita de um mesmo elemento são iguais.*

Observação 2.1.6 *É importante notarmos também que* $\overline{0}+H=\overline{3}+H$, $\overline{1}+H=\overline{4}+H$ *e* $\overline{2}+H=\overline{5}+H$. *Portanto, como são iguais, temos apenas três classes laterais distintas, que são* H, $\overline{1}+H$ *e* $\overline{2}+H$.

A seguir, relembremos a definição de ordem de um grupo, que será muito trabalhada em exemplos e proposições mais adiante.

Definição 2.1.7 *Seja* G *um grupo finito, ou seja, que contém um número finito de elementos, definimos* **ordem** *, denotada por* $|G|$, *como sendo o número de elementos de* G.

Observação 2.1.8 *De modo geral, a ordem de um conjunto é simplesmente a quantidade de elementos que ele possui.*

Exemplo 2.1.9 *Considere o grupo* $G=\mathbb{U}_{28}=\{\overline{1},\overline{3},\overline{5},\overline{9},\overline{11},\overline{13},\overline{15},\overline{17},\overline{19},\overline{23},\overline{25},\overline{27}\}$ *o conjunto dos elementos invertíveis de* $\mathbb{Z}_{28}$ *e* $H=\{\overline{1},\overline{13},\overline{15},\overline{27}\}$ *um subgrupo de ordem 4 de* G. *As classes laterais à esquerda de* H *em* G *são:*

- $\overline{1}\cdot H=\{\overline{1},\overline{13},\overline{15},\overline{27}\}$
- $\overline{3}\cdot H=\{\overline{3},\overline{11},\overline{17},\overline{25}\}$
- $\overline{5}\cdot H=\{\overline{5},\overline{9},\overline{19},\overline{23}\}$

Observação 2.1.10 *Note que* $\mathbb{U}_{28}$ *é abeliano. Logo as classes laterais à esquerda e à direita são iguais.*

Observação 2.1.11 *Assim como no exemplo 2.1.4, aqui temos apenas três classes laterais pois, as demais são iguais uma das classes laterais acima. Como por exemplo,* $\overline{9}+H=\overline{5}+H$ *e* $\overline{11}+H=\overline{3}+H$.

A seguir temos algumas proposições básicas de classes laterais.

Proposição 2.1.12 *Sejam* $(G,*)$ *um grupo,* H *um subgrupo de* G *e* $x,y\in G$. *Temos que* $y\in xH\Leftrightarrow yH=xH$.

Vejamos o exemplo a seguir.

Exemplo 2.1.13 *Tomando o grupo* $\mathbb{Z}_6$ *e o subgrupo* $H=\{\overline{0},\overline{3}\}$ *de* $\mathbb{Z}_6$. *Vejamos os seguintes casos*

- $\overline{0} \in \overline{3} + H \Leftrightarrow \overline{0} + H = \overline{3} + H$
- $\overline{1} \in \overline{4} + H \Leftrightarrow \overline{1} + H = \overline{4} + H$
- $\overline{2} \in \overline{5} + H \Leftrightarrow \overline{2} + H = \overline{5} + H$

Observando o exemplo 2.1.4, vemos que as implicações acima são válidas e portanto temos um exemplo da proposição anterior.

Proposição 2.1.14 *Para todo x, y pertencentes à um grupo G:*

$$xH = yH \Leftrightarrow y^{-1}x \in H.$$

Proposição 2.1.15 *Sejam xH e yH duas classes laterais módulo H, ou seja, que dependem de H. Temos que $xH \cap yH = \emptyset$ ou $xH = yH$. Logo, se tivermos pelo menos um elemento na interseção, as classes são iguais.*

Proposição 2.1.16 *Sejam $x_1, x_2, x_3, ..., x_k \in G$, tais que*

$$G = x_1H \bigcup x_2H \bigcup x_3H \bigcup ... \bigcup x_kH.$$

Dado um grupo finito G e um subgrupo H de G, $\exists$ n, de modo que a união de todas as classes laterais módulo H resulta no próprio G.

Proposição 2.1.17 *Seja G um grupo finito, toda classe lateral xH é equipotente à H, ou seja, todas as classes laterais possuem o mesmo número de elementos que H. Em outras palavras*

$$|xH| = |H|, \ \forall \ x \in G,$$

isto é, o número de elementos de xH é igual a ordem de H.

Nota: A partir das proposições acima, podemos concluir que o conjunto das classes laterais, módulo H, formam uma partição em G, com a característica de que aqui as classes são conjuntos equipotentes, ou seja, com a mesma cardinalidade.

Lema 2.1.18 *Considere a aplicação*

$$\begin{aligned} \varphi : \{classes\ laterais\ à\ esquerda\} &\to \{classes\ laterais\ à\ direita\} \\ xH &\mapsto Hx^{-1} \end{aligned}$$

Então φ é uma bijeção.

Definição 2.1.19 *Se o conjunto das classes laterais à esquerda de H em G é finito, o número de classes laterais à esquerda é igual ao número de classes laterais à direita, pelo Lema 2.1.18. Chamaremos de* **índice** *de H em G o número de classes laterais módulo H em G denotado por (G : H).*

A seguir, para melhor entender o que é o índice de um subgrupo, traremos alguns exemplos.

Exemplo 2.1.20 *Tomemos o grupo aditivo $\mathbb{Z}_6$ e consideremos o subgrupo $H = \{\overline{0}, \overline{2}, \overline{4}\}$. As classes laterais, à esquerda ou à direita, pois $\mathbb{Z}_6$ é comutativo, são:*

$$\overline{0} + H = \{\overline{0}, \overline{2}, \overline{4}\} \quad e \quad \overline{1} + H = \{\overline{1}, \overline{3}, \overline{5}\}.$$

Note que as outras classes laterais que poderiam ser construídas coincidem com uma das classes acima, como por exemplo, $\overline{2} + H = \overline{0} + H = \{\overline{0}, \overline{2}, \overline{4}\}$.

Logo, como a partição de $\mathbb{Z}_6$ neste caso é feita por duas classes, cada uma com 3 elementos, temos que $(\mathbb{Z}_6 : H) = 2$, ou seja, o índice de H em $\mathbb{Z}_6$ é 2.

Exemplo 2.1.21 *Retomando o exemplo 2.1.4, vemos que a partição de $\mathbb{Z}_6$ é feita por três classes laterais, cada uma com dois elementos. Dessa forma, $(\mathbb{Z}_6 : H) = 3$, ou seja, o índice de H em $\mathbb{Z}_6$ é três.*

Exemplo 2.1.22 *Observando o exemplo 2.1.9, vemos que a partição de $\mathbb{U}_{28}$ é feita por três classes laterais, cada uma com quatro elementos. Portanto, $(\mathbb{U}_{28} : H) = 3$, ou seja, o índice de H em $\mathbb{U}_{28}$ é três.*

2.2 Teorema de Lagrange

Nesta seção falaremos sobre o Teorema de Lagrange e alguns corolários, considerando grupos finitos.

Definição 2.2.1 (Teorema de Lagrange) *Seja G um grupo finito e H um subgrupo de G. Então*

$$| G | = | H | (G : H).$$

Em particular, a ordem e o índice de H dividem a ordem de G.

A seguir vejamos um exemplo no qual o Teorema de Lagrange é utilizado para encontrar todos os subgrupos de S_6.

Exemplo 2.2.2 *Procure todos os subgrupos de S_6 com suas ordens.*

Solução. *O grupo S_6 tem 6 elementos. Um subgrupo H de S_6 , pelo Teorema de Lagrange, só pode ter $\mid H \mid \in \{1, 2, 3\}$, que são os divisores de 6.*

- *O único subgrupo de ordem 1 é $\{id\}$.*
- *Os subgrupos de ordem 2 são:*

  $< (2\,3) >= \{id, (2\,3)\}$, $< (1\,3) >= \{id, (1\,3)\}$, $< (1\,2) >= \{id, (1\,2)\}$.
- *O único subgrupo de ordem 3 é $< (1\,2\,3) >= \{id, (1\,2\,3), (1\,3\,2)\} =< (1\,3\,2) >$.*

Observação 2.2.3 *A recíproca do Teorema de Lagrange é verdadeira apenas para alguns grupos, como por exemplo todos os grupos cíclicos. No entanto, em geral é falsa, pois, dado um divisor n da ordem de um grupo G, não existe necessariamente um subgrupo H de G com ordem n.*

Vejamos um exemplo em que a recíproca do Teorema de Lagrange não é válida.

Exemplo 2.2.4 *O grupo A_4, que contém as permutações pares de S_4, possui 12 elementos, que são:*

$$A_4 = \{id, (1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (2\,3\,4), (2\,4\,3), (1\,3\,4), (1\,4\,3), (1\,2)(3\,4), (1\,3)(2\,4), (2\,3)(1\,4)\}.$$

Logo, a ordem de A_4 é 12. No entanto, esse grupo não possui nenhum subgrupo de ordem 6, apesar de 6 ser um divisor da ordem de A_4.

Corolário 2.2.5 *Sejam G um grupo finito e K, H subgrupos de G, com $K \subset H$. Então*

$$(G : K) = (G : H) \cdot (H : K).$$

A seguir, relembremos a definição de ordem de um elemento de um grupo.

Definição 2.2.6 *Sejam G um grupo e $x \in G$. Dizemos que:*

- *x tem ordem finita se existe $n \in \mathbb{Z}^+$ tal que $x^n = e$. Sendo assim, o menor inteiro positivo n que obedece a essa condição é chamado de* **ordem** *de x.*
- *x tem ordem infinita caso não exista $n \in \mathbb{Z}^+$ tal que $x^n = e$.*

Corolário 2.2.7 *Sejam G um grupo finito e α um elemento de G. Então a ordem de α divide a ordem de G.*

Corolário 2.2.8 *Sejam G um grupo finito de ordem n e $\alpha \in G$, então $\alpha^n = e$.*

Corolário 2.2.9 *Seja G um grupo de ordem prima p. Então G é cíclico e seus únicos subgrupos são os triviais: G e $\{e\}$.*

2.3 Subgrupos Normais e Grupos Quocientes

Vimos até aqui que dado um grupo G podemos encontrar uma partição de G em classes laterais do subgrupo H. Nessa seção, estudaremos a estrutura das classes laterais e a relação entre elas. Veremos também que é possivel formar grupos de classes laterais, denominados de grupos quocientes.

2.3.1 Subgrupos Normais

Definição 2.3.1 *Seja H um subgrupo de G. Dizemos que H é um* **subgrupo normal** *de G (escrevemos $H \triangleleft G$) se $xH = Hx$ para todo $x \in G$, ou seja, as classes laterais à esquerda de H são iguais as classes laterais à direita de H.*

Observação 2.3.2 *O significado de $H \triangleleft G$, é que dado $x \in G$ e $h \in H$, existem $h', h'' \in H$ tal que*

$$xh = h'x \quad e \quad hx = xh''.$$

Note que o fato de H ser um subgrupo normal de G não implica em $xh = hx$, $\forall\, h \in H$.

Para melhor entender o que são os subgrupos normais, vejamos alguns exemplos a seguir.

Exemplo 2.3.3 *Seja G um grupo, os subgrupos triviais de G, $\{e\}$ e G são subgrupos normais de G.*

Definição 2.3.4 *Se os únicos subgrupos normais de G forem os triviais, dizemos que G é um* **grupo simples** *.*

Exemplo 2.3.5 *Seja G um grupo abeliano, todo subgrupo H de G é subgrupo normal. No entanto, a recíproca em geral é falsa. O grupo Q_3, grupo dos quaternios com 8 elementos, por exemplo, não é abeliano apesar de todos seus subgrupos serem normais.*

Antes do próximo exemplo, vejamos a definição de centro de um grupo.

Definição 2.3.6 *Sejam G um grupo e $x \in G$. O centro de G é o conjunto definido como $Z(G) = \{h \in G \ ; \ x.h = h.x \ \forall \ x \in G\}$, ou seja, esse conjunto é composto pelos elementos de G que comutam com todos os outros.*

Exemplo 2.3.7 *Não é difícil mostrar que $Z(G)$ é um subgrupo de G. Além disso, $Z(G)$ é sempre normal à G, pois, como vimos na definição acima, teremos $xh = hx, \forall \ x \in G$ e $\forall \ h \in Z(G)$.*

Teorema 2.3.8 *Se H é subgrupo de G e $(G : H) = 2$, então $H \triangleleft G$, ou seja, H é subgrupo normal de G.*

Teorema 2.3.9 (Teste para subgrupos normais) *Se H é subgrupo de G e $x \in G$, $H \triangleleft G \Leftrightarrow xHx^{-1} \subseteq H$.*

2.3.2 Grupos Quocientes

Nesta seção construiremos uma operação binária no conjunto das classes laterais ${}^{G}\!/_{H}$, a fim de torná-lo um grupo.

Definição 2.3.10 *Sejam G um grupo e H um subgrupo normal de G. Denotamos por*

$$ {}^{G}\!/_{H} = \{xH; \ x \in G\} $$

o conjunto das classes laterais à esquerda de H com relação à G.

Note que, como H é um subgrupo normal de G, $xH = Hx$. Logo, $xH = Hx$, ou seja, o conjunto das classes laterais à esquerda de H com relação à G é igual ao conjunto das classes laterais à direita de H com relação a G. Vamos definir a seguinte operação no conjunto das classes laterais ${}^{G}\!/_{H}$:

$$ \psi : {}^{G}\!/_{H} \times {}^{G}\!/_{H} \to {}^{G}\!/_{H} $$

dada por

$$ xH \cdot yH \mapsto (xy)H $$

Precisamos verificar se a operação ψ é bem definida, ou seja, se não depende da escolha dos representantes de x e y das classes laterais xH e yH respectivamente.

Suponha que $x, x', y, y' \in G$ são tais que $xH = x'H$ e $yH = y'H$. Então, $x' = xh_1$ e $y' = yh_2$ para algum $h_1, h_2 \in H$. Então

$$\begin{aligned}
\psi(x'H, y'H) &= (x'y')H && \textit{pela definição de } \psi \\
&= (xh_1yh_2)H \\
&= xh_1yH && \textit{pois } h_2 \in H \\
&= xh_1Hy && \textit{pois } H \textit{ é normal} \\
&= xHy && \textit{pois } h_1 \in H \\
&= xyH && \textit{pois } H \textit{ é normal} \\
&= \psi(xH, yH)
\end{aligned}$$

Portanto, a operação ψ em ${}^{G}\!/_{H}$ é bem definida. Além disso, sejam $xH,\ yH, wH \in {}^{G}\!/_{H}$, temos que as seguintes propriedades são satisfeitas.

- **(Associatividade)** $(xH \cdot yH) \cdot wH = (xy)H \cdot wH = ((xy)w)H = (x(yw))H = xH \cdot (yw)H = xH \cdot (yH \cdot wH)$.

- **(Elemento Neutro)** O elemento neutro do conjunto das classes laterais ${}^{G}\!/_{H}$ é o próprio $H = eH$, onde e é o elemento neutro do grupo G. Veja que $xH \cdot H = xH \cdot eH = (xe)H = xH$.

- **(Elemento Simétrico)** Para cada classe aH, como G é grupo, $\exists\ a^{-1} \in G$, tal que $aa^{-1} = a^{-1}a = e$. Desse modo, $aH \cdot a^{-1}H = (aa^{-1})H = eH = H$.

Portanto, como o conjunto das classes laterais ${}^{G}\!/_{H}$ satisfaz as condições que definem um grupo, concluimos que ele é também um grupo.

Definição 2.3.11 *Seja G um grupo e H um subgrupo normal de G. O conjunto das classes laterais ${}^{G}\!/_{H}$ munido da operação ψ construída anteriormente, é chamado de* **grupo quociente** *de G módulo H.*

A seguir, veremos qual a ordem de um grupo quociente e de um elemento de um grupo quociente.

Proposição 2.3.12 *Sejam G um grupo finito e H um subgrupo normal de G. Então*

$$|\ {}^{G}\!/_{H}\ | = \tfrac{|G|}{|H|}.$$

Observação 2.3.13 *Podemos definir a ordem $\mid xH \mid$, de duas maneiras:*

- *a ordem de xH como elemento de ${}^{G}/_{H}$*
- *o comprimento do conjunto xH*

É importante saber qual dos casos considerar a depender do contexto.

Proposição 2.3.14 *Sejam $H \triangleleft G$ e $x \in G$. Então, a ordem de xH em ${}^{G}/_{H}$ é o menor inteiro positivo n tal que $x^n \in H$.*

Proposição 2.3.15 *Sejam G um grupo e N um subgrupo normal de G. Temos que:*

- *Se G é um grupo abeliano, então o grupo quociente ${}^{G}/_{N}$ é um grupo abeliano.*
- *Se G é um cíclico, então o grupo quociente ${}^{G}/_{N}$ é um grupo cíclico.*

Lema 2.3.16 *Se G é um grupo e Z(G) é o centro de G, tal que ${}^{G}/_{Z(G)}$ é cíclico, então G é abeliano.*

Proposição 2.3.17 *Seja G um grupo e Z(G) seu centro. Se ${}^{G}/_{Z(G)}$ é cíclico, então Z(G)=G. Em particular, o índice de Z(G) em G nunca será primo.*

É importante mencionar que o núcleo de qualquer homomorfismo é sempre um subgrupo normal. Dessa forma, a seguir veremos um teorema muito importante, não somente na estrutura de grupos quocientes, como também nas demais estruturas que serão estudadas mais adiante.

Teorema 2.3.18 (Primeiro Teorema do Isomorfismo) *Sejam G e J grupos e $\overline{\Phi} : G \to J$ um homomorfismo de grupos. Então a aplicação*

$$\Phi : {}^{G}/_{Nuc(\overline{\Phi})} \to Im(\overline{\Phi}), \text{ definida por } \Phi(x.Nuc(\overline{\Phi})) = \overline{\Phi}(x)$$

é um isomorfismo de grupos. Em particular

$${}^{G}/_{Nuc(\overline{\Phi})} \cong Im(\overline{\Phi})$$

Demonstração: Chamaremos o núcleo de $\overline{\Phi}$ de N. Assim, queremos mostrar que a aplicações $\Phi : {}^{G}/_{N} \to Im(\overline{\Phi})$ é um isomorfismo de grupos.

Inicialmente mostraremos que Φ está bem definida. Assim, precisamos verificar que se $x' \in xN$, então $\Phi(xN) = \Phi(x'N)$. Note que, se $x' \in xN$, então $x' = xn$, para algum $n \in N$. Portanto:

- $\Phi(x'N) = \overline{\Phi}(x') = \overline{\Phi}(xn) = \overline{\Phi}(x)\overline{\Phi}(n) = \overline{\Phi}(x) \cdot e' = \overline{\Phi}(x) = \Phi(xN)$.

Em seguida, mostraremos que esta aplicação é um homomorfismo grupos.

- $\Phi(xN \cdot yN) = \Phi(xy \cdot N) = \overline{\Phi}(x \cdot y) = \overline{\Phi}(x) \cdot \overline{\Phi}(y) = \Phi(xN) \cdot \Phi(yN)$

Logo, Φ é um homomorfismo e resta mostrar que é também injetora e sobrejetora.

- $\overline{\Phi}(x) = \overline{\Phi}(x') \Rightarrow \overline{\Phi}(x) - \overline{\Phi}(x') = 0_J \Rightarrow \overline{\Phi}(x - x') = 0_J \Rightarrow x - x' \in N \Rightarrow xN = x'N$. Logo, Φ é injetora.
- Seja $y \in Im(\overline{\Phi})$, então existe $x \in G$, tal que $y = \overline{\Phi}(x)$. Considerando a classe de equivalência $x \cdot N \in {}^{G}\!/_{N}$, $\Phi(x \cdot N) = \overline{\Phi}(x) = y$. Logo, Φ é sobrejetora.

Assim, como a aplicação Φ um homomorfismo bijetor, concluimos que Φ é um isomorfismo de grupos. ■

Exemplo 2.3.19 *Seja S_n o grupo de permutações de $\{1, 2, 3, \ldots, n\}$ e A_n o subgrupo de permutações pares de S_n. A aplicação definida por $sgn : S_n \to \{1, -1\}$ é*

- *um homomorfismo com $Nuc(sgn) = A_n$*
- *sgn é sobrejetora*

Portanto, pelo Primeiro Teorema do Isomorfismo, temos que

$$ {}^{S_n}\!/_{A_n} \cong \{1, -1\}. $$

Neste capítulo estudamos a construção do grupos quocientes. Inicialmente defiinimos uma relação de equivalência entre os elementos de um grupo, definimos classes laterais, falamos sobre o Teorema de Lagrange, importante teorema da teoria de grupos, e definimos subgrupos normais, fundamentais na construção dos grupos quocientes. Por fim, definimos o conjunto das classes laterais ${}^{G}\!/_{H}$, definimos uma operação nesse conjunto, que obedece às condições que definem grupo, e assim vimos que o conjunto quociente ${}^{G}\!/_{H}$ é também um grupo, o Grupo Quociente.

No próximo capítulo estudaremos a construção dos anéis quocientes e observaremos as semelhanças e diferenças dessa construção com a que vimos neste capítulo.

Capítulo 3

Anéis Quocientes

No capítulo anterior estudamos classes laterias, subgrupos normais e grupos quocientes. Neste capítulo, buscaremos entender o que são os ideais de um anel, bem como entender como são definidas as classes laterais nesse conjunto. Esse estudo inicial é de suma importância para mais à frente estudarmos a estrutura dos Anéis Quocientes.

3.1 Ideais

Nessa seção traremos a definição de subanel e ideais, que nada mais são do que subaneis especiais utilizados na construção dos anéis quocientes. Entender o que é um ideal num anel é fundamental para entender a estrutura do anel quociente.

Definição 3.1.1 *Seja A um anel e B um subconjunto não vazio de A. Dizemos que B é um* **subanel** *de A se, e somente se obedece as seguintes condições:*

- *B é fechado para as operações de adição e multiplicação em A, ou seja, $(\forall\ a, b \in A \Rightarrow a + b \in B$ e $ab \in B)$.*
- *B é também um anel, ou seja, munido das operações de adição e multiplicação de A, B obedece à todas as condições que definem um anel.*

Na proposição a seguir veremos uma forma muito mais simples de verificar se B é ou não um subanel de A. sem ter que mostrar que ele é um anel através dos axiomas

Proposição 3.1.2 *Sejam A um anel e B um subconjunto não vazio de A, B é um subanel de A se, e somente se:*

- $\forall\ a,\ b \in B \Rightarrow a - b \in B$.

- $\forall\ a,\ b \in B \rightarrow ab \in B$

Vejamos a seguir alguns exemplos de subaneis.

Exemplo 3.1.3 *O subconjunto* $2\mathbb{Z}$ *é um subanel de* $\mathbb{Z}$.

Observação 3.1.4 *De forma mais geral, os subconjuntos* $n\mathbb{Z}$ *são sempre subaneis de* $\mathbb{Z}$.

Exemplo 3.1.5 *O subconjunto*

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix};\ a, b \in \mathbb{Z} \right\}$$

é um subanel de $M_2(\mathbb{R})$.

Definição 3.1.6 *Sejam* A *um anel e* I *um subanel de* A. *Dizemos que* I *é*

- *um* **ideal** *de* A, *se* $\forall\, x \in I\ e\ a \in A \Rightarrow x.a \in I\ e\ a.x \in I$.
- *um* **ideal à direita** *de* A, *se* $\forall\, x \in I\ e\ a \in A \Rightarrow x.a \in I$.
- *um* **ideal à esquerda** *de* A, *se* $\forall\, x \in I\ e\ a \in A \Rightarrow a.x \in I$.

Observação 3.1.7 *Notemos que se* A *for um anel comutativo os ideais à direta e à esquerda são iguais.*

O Teorema a seguir estabelece as condições necessárias para que um subconjunto I de A seja ideal.

Teorema 3.1.8 *Sejam* A *um anel e* $I \neq \emptyset$ *um subconjunto de* A. I *é um* **ideal** *em* A *se, e somente se*

(i) $\forall\, x, y \in I \Longrightarrow x - y \in I$

(ii) $\forall\, x \in I\ e\ a \in A \Longrightarrow x \cdot a \in I\ e\ a \cdot x \in I$.

Exemplo 3.1.9 *No anel* $\mathbb{Z}$ *dos inteiros todos os subconjuntos* $n\mathbb{Z} = \{nq \,|\, q \in \mathbb{Z}\}$, *onde* n *é um inteiro dado, são ideais. Mostraremos inicialmente que esse conjunto é não vazio.*

- $n\mathbb{Z} \neq \emptyset$ *pois,* $0 \in n\mathbb{Z}$, *uma vez que 0=n0.*

Pelo Teorema 3.1.8, vejamos que $n\mathbb{Z}$ é um ideal em $\mathbb{Z}$.

(i) *Sejam $nq_1, nq_2 \in n\mathbb{Z}$, temos que*
$nq_1 - nq_2 = n(q_1 - q_2) \in n\mathbb{Z}$.

(ii) $\forall\ a \in \mathbb{Z}$ *e* $nq \in n\mathbb{Z},\ a(nq) = n(aq) \in n\mathbb{Z}$.

Como $\mathbb{Z}$ é um anel comutativo, os ideais à esquerda e à direita em $\mathbb{Z}$ são iguais, ou seja, $a(nq) = (nq)a$, tal que $(nq)a \in n\mathbb{Z}$.

Exemplo 3.1.10 *O subanel $m\mathbb{Z} \times n\mathbb{Z}$ é ideal em $\mathbb{Z} \times \mathbb{Z}$. Vejamos que o mesmo é não vazio.*

- $m\mathbb{Z} \times n\mathbb{Z} \neq \emptyset\, pois, (m0, n0) = (0, 0) \in m\mathbb{Z} \times n\mathbb{Z}$.

Pelo Teorema 3.1.8:

(i) *Sejam $(mq_1, nq_2), (mp_1, np_2) \in m\mathbb{Z} \times n\mathbb{Z}$ temos que*
$(mq_1, nq_2) - (mp_1, np_2) = (mq_1 - mp_1, mq_2 - mp_2) = (m(q_1 - q_2), n(p_1 - p_2)) \in m\mathbb{Z} \times n\mathbb{Z}$.

(ii) *Sejam $(mq_1, nq_2) \in m\mathbb{Z} \times n\mathbb{Z}$ e $(a, b) \in \mathbb{Z} \times \mathbb{Z}$, temos que*
$(mq_1, nq_2) \cdot (a, b) = ((mq_1)a, (nq_2)b) = (m(q_1a), n(q_2b)) \in m\mathbb{Z} \times n\mathbb{Z}$.
Como o anel $\mathbb{Z} \times \mathbb{Z}$ é abeliano, os ideais à direita e a esquerda são iguais. Logo,
$(a, b).(mq_1, nq_2) \in m\mathbb{Z} \times n\mathbb{Z}$.

Exemplo 3.1.11 *Em todo anel A, os subconjuntos $\{0\}$ e A são sempre ideais em A, chamados de* **ideais triviais** *de A. Um ideal não trivial é chamado de* **ideal próprio** .

Definição 3.1.12 *Se os únicos ideais de A forem os triviais e A for um anel com unidade, dizemos que A é um* **anel simples**.

Observação 3.1.13 *Por definição, todo ideal I num anel A é subgrupo de A. No entanto, a recíproca não é verdadeira. Por exemplo, $\mathbb{Z}$ é subgrupo de $\mathbb{Q}$, mas não é ideal em $\mathbb{Q}$. Basta notar que $1 \in \mathbb{Z}$ e $\frac{1}{2} \in \mathbb{Q}$, mas $1 \cdot \frac{1}{2} = \frac{1}{2} \cdot 1 = \frac{1}{2} \notin \mathbb{Z}$*

Proposição 3.1.14 *Seja I um ideal num anel comutativo A. Então:*

(a) $0 \in I$, *ou seja, o zero de A pertence a I;*

(b) $(\forall\, a)(a \in I \Longrightarrow -a \in I)$;

(c) $(\forall\, a, b)(a, b \in I \Longrightarrow a + b \in I)$;

(d) Se o anel A possui unidade e se existe um elemento inversível $u \in A$ tal que $u \in I$, então I=A.

3.1.1 Ideais gerados e Ideais principais

Seja A um anel comutativo com unidade. Tomemos $a_1, a_2, ..., a_n \in A\,(n \geq 1)$. Indiquemos por $< a_1, a_2, ..., a_n >$ o seguinte subconjunto de A:

$$< a_1, a_2, \dots, a_n >= \{x_1a_1 + x_2a_2 + ... + x_na_n \mid x_1, x_2, \dots, x_n \in A\}$$

Verifiquemos que o subconjunto acima é um ideal em A. Primeiramente, mostraremos que o mesmo é não vazio:

- $< a_1, a_2, \cdots, a_n > \neq \emptyset$, pois, $0 = 0a_1 + 0a_2 + \cdots + 0a_n \Longrightarrow 0 \in < a_1, a_2, \cdots, a_n >$.

Agora, verifiquemos que as condições estabelecidas no Teorema 3.1.8 são satisfeitas:

(i) Sejam $x, y \in < a_1, a_2, \cdots, a_n >$, então:

$\exists\ x_1, \cdots, x_n \in A,\ tais\ que\ x = x_1a_1 + \cdots + x_na_n$
$\exists\ y_1, \cdots, y_n \in A,\ tais\ que\ y = y_1a_1 + \cdots + y_na_n$

Daí, temos que
$x - y = (x_1 - y_1)a_1 + \cdots + (x_n - y_n)a_n \in < a_1, a_2, \cdots, a_n >$.

(ii) Seja $x \in < a_1, a_2, \cdots, a_n >$ e $b \in A$, então:

$xb = (x_1a_1 + \cdots + x_na_n)b = (x_1a_1)b + \cdots + (x_na_n)b = b(x_1a_1) + \cdots + b(x_na_n) = (bx_1)a_1 + \cdots + (bx_n)a_n \in < a_1, a_2, \cdots, a_n >$.

Como A é um anel comutativo, temos que bx = xb, ou seja, os ideais à direita são iguais aos ideais à esquerda.

Portanto, como todas as condições necessárias são satisfeitas, concluimos que o subconjunto $< a_1, a_2, \cdots, a_n >$ é ideal em A.

Definição 3.1.15 *O ideal* $< a_1, a_2, \cdots, a_n >$ *obtido segundo as considerações acima é chamado de* **ideal gerado** *por* $a_1, a_2, \cdots, a_n$.

Definição 3.1.16 *Chamamos de* **ideal principal** *um ideal I gerado por um único elemento* $a \in A$, *ou seja,* $I = < a >$.

Observação 3.1.17 *Quando tratamos de ideais principais, além da notação* $< a >$, *usamos também a notação aA. Note que essa última foi usada no exemplo 3.1.9 quando falamos de ideais em* $\mathbb{Z}$.

Teorema 3.1.18 *Seja* $A = \mathbb{Z}$ *ou* $\mathbb{Z}_m$ *para algum* $m \in \mathbb{Z}_+$. *Então*

os subgrupos de (A,+) = subaneis de A = ideais de A

Além disso, todo ideal em A é principal.

Vejamos a seguir um exemplo que ilustra esse teorema.

Exemplo 3.1.19 *No anel* $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$*, os ideais são os seguintes:*

- $I_1 = \{0\}$
- $I_2 =< 1 >= 1\mathbb{Z}_6 = \mathbb{Z}_6$
- $I_3 =< 2 >= 2\mathbb{Z}_6 = \{\overline{0}, \overline{2}, \overline{4}\}$
- $I_4 =< 3 >= 3\mathbb{Z}_6 = \{\overline{0}, \overline{3}\}$
- $I_5 =< 4 >= 4\mathbb{Z}_6 = \{\overline{0}, \overline{2}, \overline{4}\}$
- $I_6 =< 5 >= 5\mathbb{Z}_6 = \mathbb{Z}_6$

Como $\mathbb{Z}_6$ é um anel comutativo, não há diferença entre os ideais à esquerda e à direita. Além disso, o teorema anterior nos diz que os ideais de $\mathbb{Z}_6$ são principais e iguais aos subgrupos e subaneis de $\mathbb{Z}_6$.

3.1.2 Ideais Primos e Maximais

Definição 3.1.20 *Seja P um ideal num anel A. Dizemos que P é um* **ideal primo** *se* $P \neq A$ *e,*

$$\forall\ a, b \in A, ab \in P \Longrightarrow a \in P \text{ ou } b \in P$$

A seguir, vejamos alguns exemplos de ideais primos.

Exemplo 3.1.21 $\{0\}$ *em* $\mathbb{Z}$ *é primo, pois* $\{0\} \neq \mathbb{Z}$ *e* $ab \in \{0\} \Longrightarrow a \in \{0\}$ *ou* $b \in \{0\}$*.*

Exemplo 3.1.22 $2\mathbb{Z}$ *em* $\mathbb{Z}$ *é ideal primo, pois* $2\mathbb{Z} \neq \mathbb{Z}$ *e* $ab \in 2\mathbb{Z} \Longrightarrow 2|ab \Longrightarrow 2|a$ *ou* $2|b \Longrightarrow a \in 2\mathbb{Z}$ *ou* $b \in 2\mathbb{Z}$*.*

Exemplo 3.1.23 *O ideal* $\{0\} \times \mathbb{Z}$ *em* $\mathbb{Z}$ *é primo, pois além de ser diferente de* $\mathbb{Z} \times \mathbb{Z}$*, temos que:*
(a,b)(c,d) $\in \{0\} \times \mathbb{Z} \Longrightarrow (ac, bd) \in \{0\} \times \mathbb{Z} \Longrightarrow ac = 0 \Longrightarrow a = 0$ *ou* $c = 0 \Longrightarrow (a, b) \in \{0\} \times \mathbb{Z}$ *ou* $(c, d) \in \{0\} \times \mathbb{Z}$*.*

Notemos que $\mathbb{Z} \times \{0\}$ *em* $\mathbb{Z} \times \mathbb{Z}$ *também é ideal primo. Podemos mostrar isso de forma semelhante a anterior, considerando* $bd = 0$*.*

Exemplo 3.1.24 *Em* $\mathbb{Z}$*, o ideal*

$$< m >= m\mathbb{Z} = \begin{cases} \text{é ideal primo} & \text{, se } m \text{ é um número primo} \\ \text{não é ideal primo} & \text{, se } m \text{ não for um número primo} \end{cases}$$

De fato, se é m um número composto, ou seja, que não é primo, tal que $m = abcoma, b > 1$*, então* $ab \in m\mathbb{Z}$*, mas* $a, b \notin m\mathbb{Z}$*. Assim, concluimos que* $m\mathbb{Z}$ *não é primo. Por exemplo,* $< 6 >= 6\mathbb{Z}$ *não é primo, pois*

$$6 = 2 \cdot 3 \in 6\mathbb{Z}, \text{ mas } 2 \notin 6\mathbb{Z} e\ 3 \notin 6\mathbb{Z}.$$

No entanto, se $m = p$ *é primo e* $ab \in p\mathbb{Z} \Longrightarrow p|ab \Longrightarrow p|a$ *ou* $p|b \Longrightarrow a \in p\mathbb{Z}$ *ou* $b \in p\mathbb{Z}$*. Logo,* $p\mathbb{Z}$ *é um ideal primo em* $\mathbb{Z}$*.*

Definição 3.1.25 *Seja A um anel comutativo e M um ideal em A. Dizemos que M é* **ideal maximal** *se* $M \neq A$ *e não existir nenhum ideal N em A, tal que* $M \subseteq N \subseteq A$*. Ou seja, M é ideal maximal se o único ideal em A que contém M, e é diferente de M, for o próprio A. Em outras palavras, dizemos que M é um elemento maximal em relação à inclusão, no conjunto dos ideais em A diferentes de A.*

A seguir, vejamos alguns exemplos de ideais maximais e ideais não maximas.

Exemplo 3.1.26 *No exemplo 3.1.21, vimos que* $\{0\}$ *é um ideal primo em* $\mathbb{Z}$*. No entanto, de forma simples percebemos* $\{0\}$ *não é ideal maximal de* $\mathbb{Z}$*, pois*

$$\{0\} \subseteq 2\mathbb{Z} \subseteq \mathbb{Z}.$$

Exemplo 3.1.27 $2\mathbb{Z}$ *em* $\mathbb{Z}$ *é ideal maximal pois* $2\mathbb{Z} \subseteq \mathbb{Z}$ *e se N é ideal em* $\mathbb{Z}$ *e* $N \supset 2\mathbb{Z}$ *então* $1 \in N$ *e* $N = \mathbb{Z}$*.*

Exemplo 3.1.28 $p\mathbb{Z}$*, com p primo, é um ideal maximal em* $\mathbb{Z}$*. Por exemplo,* $3\mathbb{Z} \subset \mathbb{Z}$ *é ideal maximal em* $\mathbb{Z}$*, pois, se N é ideal em* $\mathbb{Z}$*, tal que* $3\mathbb{Z} \subseteq N \subseteq \mathbb{Z}$*, então* $N = \mathbb{Z}$*. Logo, precisamos mostrar que* $1 \in N$*. Como* $3\mathbb{Z} \subseteq N$*, existe* $a \in N$ *não divisível por* 3*. Portanto, a e* 3 *são coprimos e* $3n + am = 1$ *para alguns* $n, m \in \mathbb{Z}$*. Portanto* $1 \in N$*.*

Exemplo 3.1.29 *Seja m um inteiro positivo composto. Então $m\mathbb{Z}$ não é maximal pois*

$$6\mathbb{Z} \subset 2\mathbb{Z} \subset \mathbb{Z} \text{ e também } 6\mathbb{Z} \subset 3\mathbb{Z} \subset \mathbb{Z}.$$

3.2 Anéis Quocientes

Agora que já sabemos o que são ideais podemos iniciar nossos estudos sobre Anéis Quocientes. Nessa seção, primeiramente veremos a relação de equivalência e as classes laterais em um Anel, as operações de adição e multiplicação no conjunto quociente para em seguida definir Anel Quociente e estudar alguns teoremas que o envolvem.

3.2.1 Conceito de Anel Quociente

Assim como fizemos para Grupos Quocientes, definiremos agora uma relação de equivalência determinada pelo ideal I sobre o anel A.

Definição 3.2.1 *Seja A um anel e I um ideal em A. Para todo $x, y \in A$, podemos estabelecer a seguinte relação:*

$$x \sim y \Leftrightarrow x - y \in I.$$

A relação acima é de fato uma relação de equivalência sobre A, pois

1. $0 \in I \Rightarrow x - x \in I \Rightarrow x \sim x$ $(\forall\ x \in A)$ (Reflexiva);
2. $x \sim y \Rightarrow x - y \in I \Rightarrow -(x - y) \in I \Rightarrow y - x \in I \Rightarrow y \sim x$ (Simétrica);
3. $x \sim y$ *e* $y \sim z \Rightarrow x - y \in I$ *e* $y - z \in I \Rightarrow (x - y) + (y - z) \in I \Rightarrow x - z \in I \Rightarrow x \sim z$ (Transitiva).

Definição 3.2.2 *Seja I um ideal num anel A. Seja $a \in A$. Definimos a* **classe lateral** *de a como sendo o conjunto*

$$a + I = \{a + i;\ i \in I\}.$$

Observação 3.2.3 *A classe definida acima é chamada de classe lateral determinada por a, módulo I, em A. Também é chamada de classe de equivalência em A com respeito à relação de equivalência da definição 3.2.1 e a indicada por $\bar{a}$, então $\bar{a} = a + I$.*

Definição 3.2.4 *Chamamos de conjunto quociente, denotado por A/I, o conjunto das classes de equivalência $\sim$, ou seja*

$$^{A}/_{I} = \{a + I;\ a \in A\}.$$

Notemos que a proposição a seguir é semelhante a proposição 2.1.15, na página 14, que envolvia as classes laterais de grupo.

Proposição 3.2.5 *Seja I um ideal em um anel A. Para quaisquer $a, b \in A$ temos que*

$$(a + I) \cap (b + I) = \emptyset \text{ ou } a + I = b + I$$

Além disso, $a + I = b + I \Rightarrow a - b \in I$.

A seguir, veremos que podemos definir as operações de adição e multiplicação no conjunto das classes laterais $^{A}/_{I}$.

Adição em $^{A}/_{I}$

A expressão a seguir define uma lei de composição interna em $^{A}/_{I}$

$$(a + I) + (b + I) = (a + b) + I, \forall\, a, b \in A.$$

Vejamos que essa operação está bem definida, ou seja, não depende da escolha dos representantes das classes de equivalência.

Se $a + I = a' + I$ *e* $b + I = b' + I$, então existem x_1 *e* $x_2 \in I$ tais que $a = a' + x_1$ e $b = b' + x_2$

$$\begin{aligned}
(a + I) + (b + I) &= (a + b) + I \\
&= ((a' + x_1) + (b' + x_2)) + I \\
&= ((a' + b') + (x_1 + x_2)) + I \\
&= (a' + b') + I + (x_1 + x_2) + I \\
&= (a' + b') + I \\
&= (a' + I) + (b' + I) \\
&= (a + I) + (b + I).
\end{aligned}$$

Essa lei de composição interna é a adição em $^{A}/_{I}$.

Relativamente a essa adição, o conjunto $^{A}/_{I}$ é um grupo abeliano, ou seja, um grupo comutativo. De fatoo, sejam $a + I, b + I, c + I \in {}^{A}/_{I}$ as seguintes condições são válidas:

- **(Associatividade)** (a + I) + [(b + I) + (c + I)] = (a + I) + [(b + c) + I] = [a + (b + c)] + I = [(a + b) + c] + I = [(a + b) + I] + (c + I) = [(a + I)+(b + I)] + (c + I).

- **(Elemento Neutro)** O elemento neutro das classes de equivalência é a classe $0 + I = I$, ou seja, o próprio I.

- **(Oposto)** Para cada classe $a + I$ a classe $(-a) + I$ é o elemento oposto de $a + I$, pois $(a + I) + (-a + I) = (a - a) + I = 0 + I = I$.
  Logo, -(a + I) = (-a) + I.

- **(Comutatividade)** $(a + I) + (b + I) = (a + b) + I = (b + a) + I = (b + I) + (a + I)$

Multiplicação em $^{A}/_{I}$

A expressão a seguir define uma lei de composição interna em $^{A}/_{I}$:

$$(a + I) \cdot (b + I) = a \cdot b + I, \forall\ a, b \in A.$$

Vejamos que essa operação também está bem definida. Logo, assim como fizemos para a operação anterior, consideremos que se $a + I = a' + I$ *e* $b + I = b' + I$, então existem x_1 *e* $x_2 \in I$ tais que $a = a' + x_1$ e $b = b' + x_2$

$$\begin{aligned}
(a + I) \cdot (b + I) &= a \cdot b + I \\
&= (a' + x_1)(b' + x_2) + I \\
&= (a' \cdot b' + a' \cdot x_2 + x_1 \cdot b' + x_1 \cdot x_2) + I \\
&= (a' \cdot b' + I) + ((\underbrace{a' \cdot x_2 + x_1 \cdot b' + x_1 \cdot x_2}_{\in I}) + I), \text{pois I é ideal.} \\
&= a' \cdot b' + I \\
&= (a' + I) \cdot (b' + I) \\
&= (a + I) \cdot (b + I).
\end{aligned}$$

Essa lei de composição é a multiplicação em $^{A}/_{I}$, e apresenta as seguintes propriedades:

- **(Associatividade)** $(a + I) \cdot [(b + I) \cdot (c + I)] = (a + I) \cdot (b \cdot c + I) = (a \cdot (b \cdot c) + I) = ((a \cdot b) \cdot c + I) = (a \cdot b + I) \cdot (c + I) = [(a + I) \cdot (b + I)] \cdot (c + I)$.

- **(Distributividade)** $(a + I) \cdot [(b + I) + (c + I)] = (a + I) \cdot [(b + c) + I] = a \cdot (b + c) + I = (a \cdot b + a \cdot c) + I = (a \cdot b + I) + (a \cdot c + I) = (a + I) \cdot (b + I) + (a + I) \cdot (c + I)$.

Portanto, como o conjunto $^{A}/_{I}$ obedece as condições que definem um anel, concluimos que este é um anel em relação à adição e à multiplicação.

Definição 3.2.6 *Sejam A um anel e I um ideal em A. O anel ${}^{A}\!/_{I}$, introduzido pelas considerações acima, é chamado de* **anel quociente** .

Observação 3.2.7 *Se o anel A possui unidade, o anel ${}^{A}\!/_{I}$ também possui, sendo essa a classe $1 + I$, na qual 1 indica a unidade do anel A. Portanto, $({}^{A}\!/_{I}, +, \cdot)$ é também um anel com unidade se A for um anel com unidade.*

Teorema 3.2.8 (Primeiro Teorema do Isomorfismo) *Sejam A e B anéis e $\bar{\varphi} : A \to B$ um homomorfismo de anéis. Então a aplicação:*

$$\varphi : {}^{A}\!/_{Nuc(\bar{\varphi})} \to Im(\bar{\varphi}),\ \textit{definida por}\ \varphi(a + Nuc(\bar{\varphi})) = \bar{\varphi}(a)$$

é um isomorfismo de anéis. Em particular

$${}^{A}\!/_{Nuc(\bar{\varphi})} \ \cong\ Im(\bar{\varphi}).$$

Demonstração:

Chamaremos o núcleo de $\bar{\varphi}$ de N. Assim, queremos mostrar que a aplicação $\varphi : {}^{A}\!/_{N} \to Im(\bar{\varphi})$ é um isomorfismo de anéis.

Inicialmente mostraremos que esta aplicação é um homomorfismo de anéis:

- $\varphi((a+N)+(b+N)) = \varphi((a+b)+N) = \bar{\varphi}(a+b) = \bar{\varphi}(a) + \bar{\varphi}(b) = \varphi(a+N) + \varphi(b+N)$
- $\varphi((a+N)\cdot(b+N)) = \varphi((a\cdot b+N)) = \bar{\varphi}(a\cdot b) = \bar{\varphi}(a)\cdot\bar{\varphi}(b) = \varphi(a+N)\cdot\varphi(b+N)$

Logo, φ é um homomorfismo de anéis, e resta mostrar que é também bijetora.

- $\bar{\varphi}(a) = \bar{\varphi}(a') \Rightarrow \bar{\varphi}(a) - \bar{\varphi}(a') = 0_B \Rightarrow \bar{\varphi}(a-a') = 0_B \Rightarrow a - a' \in N \Rightarrow a + N = a' + N$. Logo, φ é injetora.
- Seja $b \in Im(\bar{\varphi})$. Então, $\exists\ a \in A$, tal que, $b = \bar{\varphi}(a)$. Tome $a + N \in {}^{A}\!/_{N}$. Daí, $\varphi(a+N) = \bar{\varphi}(a) = b$. Logo, φ é sobrejetora.

Assim, como a aplicação φ é um homomorfismo bijetor, então concluimos que é um isomorfismo de anéis. ■

Vejamos os exemplos a seguir que aplicam esse teorema.

Exemplo 3.2.9 ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \cong \mathbb{Z}_n$, *pois $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, definida por $\varphi(a) = \bar{a}$, é um homomorfismo sobrejetor com $Nuc(\varphi) = n\mathbb{Z}$*

Observação 3.2.10 *Observe no exemplo anterior que o anel $\mathbb{Z}$ é infinito, e ao quocientarmos ele pelo anel $n\mathbb{Z}$, que também é infinito, temos que esse quociente é isomorfo à $\mathbb{Z}_n$, que por sua é vez finito. Essa seria uma vantagem do quociente em anéis, pegar algo que é infinito e ver que é isomorfo à algo finito.*

Exemplo 3.2.11 $\frac{M_2(\mathbb{Z})}{M_2(n\mathbb{Z})} \cong M_2(\mathbb{Z}_n)$, *pois* $\varphi : M_2(\mathbb{Z}) \to M_2(\mathbb{Z}_n)$ *definido por*

$$\varphi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix},$$

é um homomorfismo de anéis sobrejetor, com

$$Ker(\varphi) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}); \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} = \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{0} \end{pmatrix} \right\}.$$

Agora,

$$\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} = \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{0} \end{pmatrix} \Leftrightarrow \bar{a} = \bar{b} = \bar{c} = \bar{d} = \bar{0}, \textit{ou seja, } a,\ b,\ c,\ d \in n\mathbb{Z},$$

o que implica que

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}).$$

Portanto, $Nuc(\varphi) \subseteq M_2(\mathbb{Z})$ e, a inclusão contrária é obvia. O que mostra que $\frac{M_2(\mathbb{Z})}{M_2(n\mathbb{Z})} \cong M_2(\mathbb{Z}_n)$.

Homomorfismo Canônico

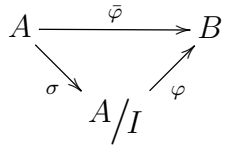
Seja A um anel e I um ideal de A. A aplicação $\sigma : A \to {}^{A}\!/_{I}$, definida por $\sigma(a) = a + I$, para todo $a \in A$, é um homomorfismo sobrejetor de anéis com núcleo I, ou seja, todo ideal de A é núcleo de um homomorfismo de anéis com domínio A. Verifiquemos:

- $\sigma(a + b) = (a + b) + I = (a + I) + (b + I) = \sigma(a) + \sigma(b)$,
- $\sigma(a \cdot b) = (a \cdot b) + I = (a + I) \cdot (b + I) = \sigma(a) \cdot \sigma(b)$, para todo a, b $\in A$.

Assim, mostramos que a aplicação é um homomorfismo.

- É fácil verificar que a aplicação é sobrejetora, pois dada uma classe $a + I$, ela é imagem do elemento $a \in A$, pela aplicação σ. Logo, σ é sobrejetora.

O homomorfismo acima definido é chamado de **homomorfismo canônico** ou homomorfismo natural de A sobre A/I. Com ele podemos compor o seguinte diagrama de anéis e homomorfismo.



onde $\varphi \circ \sigma = \bar{\varphi}$.

A seguir, vejamos um exemplo que aplica o homomorfismo canônico definido anteriormente.

Exemplo 3.2.12 *Seja o ideal $n\mathbb{Z}$ do anel $\mathbb{Z}$, com $n \geq 0$, temos $\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z}; a \in \mathbb{Z}\}$. Dado $a \in \mathbb{Z}$, pelo Algoritmo da Divisão, temos que existem $q, r \in \mathbb{Z}$, tais que $a = qn + r$, com $0 \leq r \leq n - 1$. Assim,*

$$\begin{aligned} a + n\mathbb{Z} &= (nq + r) + n\mathbb{Z} \\ &= (nq + n\mathbb{Z}) + (r + n\mathbb{Z}) \\ &= n\mathbb{Z} + (r + n\mathbb{Z}) \\ &= r + n\mathbb{Z} \end{aligned}$$

Então, $\mathbb{Z}/n\mathbb{Z} = \{r + n\mathbb{Z};\ r = 0, 1, ..., n - 1\}$, onde $r + n\mathbb{Z} = \{r + nk;\ k \in \mathbb{Z}\} = \{b \in \mathbb{Z}; b \equiv r \ mod\ n\} = \bar{r} \in \mathbb{Z}_n$, ou seja, $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.

3.2.2 Domínio de integridade e corpo em A/I

Seja A um anel e I um ideal de A. Queremos saber quando o anel quociente A/I é um domínio de integridade ou um corpo. Veremos que isto não depende do anel A, e sim das propriedades do ideal I que vimos na seção 3.1.2, na página 26.

Teorema 3.2.13 *Seja A um anel comutativo com unidade e $I \subseteq A$ um ideal. Então*

$$A/I \text{ é um } \textbf{domínio de integridade} \Leftrightarrow I \text{ é primo.}$$

Demonstração:

($\Leftarrow$)

Suponha que I seja um ideal primo de A. Sejam $(a+I),\ (b+I) \in {}^{A}\!/_{I}$ tais que

$$(a+I).(b+I) = a.b + I = I$$

Então temos $ab \in I$. Como I é primo, temos que $a \in I$ *ou* $b \in I$, isto é, $a+I = I$ *ou* $b+I = I$. Portanto, ${}^{A}\!/_{I}$ é um domínio de integridade.

($\Rightarrow$)

Suponha que ${}^{A}\!/_{I}$ seja um domínio de integridade. Sejam $a, b \in A$, tais que $ab \in I$, isto é

$$(a.b) + I = (a+I).(b+I).$$

Por hipótese, $a+I = I$ *ou* $b+I = I$, ou seja, $a \in I$ *ou* $b \in I$. Portanto, I é ideal primo. ■

Exemplo 3.2.14 *Seja A um domínio de integridade. Então $\{0\}$ é ideal primo. Vimos que ${}^{A}\!/_{\{0\}} \cong A$ que é de fato um domínio de integridade.*

Exemplo 3.2.15 *Seja $\mathbb{Z} \times \{0\}$ um ideal primo de $\mathbb{Z} \times \mathbb{Z}$. Então temos que $\frac{(\mathbb{Z}\times\mathbb{Z})}{\mathbb{Z}\times\{0\}} \cong \mathbb{Z}$ que de fato é um domínio de integridade.*

Exemplo 3.2.16 *Seja p um número primo, então $p\mathbb{Z}$ é um ideal primo e ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \cong \mathbb{Z}_p$ é um domínio de integridade.*

Exemplo 3.2.17 *Seja n um número composto, então $n\mathbb{Z}$ não é ideal primo e ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \cong \mathbb{Z}_n$ não é um domínio de integridade.*

Teorema 3.2.18 *Seja A um anel comutativo com unidade e $M \subseteq A$. Então*

$${}^{A}\!/_{M} \text{ é um } \textbf{corpo} \Leftrightarrow M \text{ é maximal.}$$

Demonstração:

($\Rightarrow$)

Suponhamos que ${}^{A}\!/_{M}$ seja um corpo. Então, $M \neq A$ (pois, $0 \neq 1 \in {}^{A}\!/_{M}$). Agora, suponhamos que existe um ideal J *tal que* $M \subseteq J \subseteq A$. Tomando $a \in J,\ a \notin M$, então $a + M \neq M$. Como ${}^{A}\!/_{M}$ é um corpo, todo elemento diferente de M tem inverso multiplicativo, ou seja, $a+M$ é inversível. Portanto, exisite $y \in A$ tal que:

$$(a+M).(y+M) = ay + M = 1 + M$$

Logo, $ab - 1 \in M \subset J$ e, portanto, $1 = ab + x$ para algum $x \in J$. Mas $ab \in J$, pois $a \in J$ e, assim, $1 \in J$. Logo, temos que $J = A$ portanto, M é maximal.

($\Leftarrow$)
Suponha que M é maximal. Se A é anel comutativo com unidade 1_A e M é ideal maximal de A, então ${}^{A}\!/_{M}$ é um anel comutativo com $1_{A/M} = 1_A + M$.

Dado $a + M \neq M$ em ${}^{A}\!/_{M}$, temos que $a \notin M$, e assim $a + M = R$. Logo, existem $y \in A$ e $x \in M$ tais que $1 = a.y + x$. Logo, temos que

$$\begin{aligned} 1 + M &= (a.y + x) + M \\ &= (a.y + M) + (x + M) \\ &= (a.y + M) \\ &= (a + M).(y + M). \end{aligned}$$

Como ${}^{A}\!/_{M}$ é comutativo, temos que $(a + M)^{-1} = (b + M) \in {}^{A}\!/_{M}$, o que mostra que ${}^{A}\!/_{M}$ 'e, de fato, um corpo. ■

Neste capítulo analisamos a construção dos anéis quocientes. Inicialmente relembramos a definição de ideal, muito importante na construção dessa estrutura, estabelecemos uma relação de equivalência entre os elementos de um anel e definimos as classes laterais, assim como fizemos em grupos. Por fim, definimos o conjunto quociente ${}^{A}\!/_{I}$ e às operações de adição e multiplicação dentro desse conjunto, operações essas que obedecem as condições que definem anel. Dessa forma, vimos que o conjunto quociente ${}^{A}\!/_{I}$ é também um anel, o Anel Quociente.

No próximo capítulo estudaremos a construção dos espaços quocientes, e dessa vez observaremos as semelhanças e diferenças dessa construção com a dos grupos e anéis quocientes.

Capítulo 4

Espaços Quocientes

Nesse capítulo estudaremos os Espaços Quocientes, conteúdo pouco abordado nos livros de Álgebra Linear, percebendo que a construção dessa estrutura segue como a construção dos Grupos e Anéis Quocientes abordados nos capítulos anteriores.

4.1 Subespaço Vetorial e Suplementar

Na construção de grupos e anéis quocientes foi fundamental estudarmos subgrupos e subaneis especiais, os subgrupos normais e os ideais num anel. Em espaços quocientes é importante entendermos o que são subespaços vetoriais. No entanto, nessa construção trabalhamos com subespaços vetoriais quaisquer, ou seja, estes não tem uma característica especial como os subgrupos normais e os ideais.

Definição 4.1.1 *Seja V um espaço vetorial sobre um corpo F. Chamamos de* **subespaço** *de V, o subconjunto W de V que também é um espaço vetorial sobre o corpo F com as operações de adição de vetores e multiplicação escalar de V.*

Para verificar se um subconjunto W de V é um subespaço vetorial bastaria verificar se os axiomas que definem um espaço vetorial são válidos em W. No entanto, podemos tornar essa verificação mais simples utilizando o teorema a seguir.

Teorema 4.1.2 *Seja V um espaço vetorial sobre um corpo F e $W \neq \emptyset$ um subconjunto de V. Então, W é um subespaço vetorial em V se, e somente se, para cada par de vetores $\alpha,\ \beta \in W$ e cada escalar $c \in F$ o vetor $c\alpha + \beta \in W$.*

Exemplo 4.1.3 *Para todo espaço vetorial V, os subconjuntos $\{0\}$ e V são sempre subespaços vetoriais de V. São os chamados* **subespaços triviais** *ou* **impróprios**.

Exemplo 4.1.4 *$W = \{(x, y, z) \in \mathbb{R}^3 \mid x + y = 0\}$ é subespaço de $\mathbb{R}^3$. Para verificar, sejam $\alpha = (x, y, z)$ e $\beta = (x_1, y_1, z_1)$ vetores em W e c um escalar em $\mathbb{R}$.*
Temos que $c\alpha+\beta = c(x, y, z)+(x_1, y_1, z_1) = (cx, cy, cz)+(x_1, y_1, z_1) = (\underbrace{cx + x_1}_{p}, \underbrace{cy + y_1}_{q}, cz+z_1)$.
Note que, $p + q = (cx + x_1) + (cy + y_1) = (cx + cy) + (x_1 + y_1) = c(x + y) + (x_1 + y_1) = c.0 + 0 = 0 + 0 = 0$. Logo, como $p + q = 0$, $c\alpha + \beta \in W$. Portanto, pelo Teorema 4.1.2, W é um subespaço vetorial de $\mathbb{R}^3$.

Exemplo 4.1.5 *A interseção entre dois subespaços de um mesmo espaço vertorial V é também um subespaço vetorial de V. Para verificar isso, sejam U e W subespaços vetoriais de V sobre o corpo F, u e w vetores, tais que $u, w \in U \cap W \Rightarrow u, w \in U$ e $u, w \in W$, e c um escalar em F. Note que, $cu + w \in U \cap W$, pois $cu + w \in U$ e $cu + w \in W$ já que U e W são subespaços de V. Logo, pelo Teorema 4.1.2, $U \cap W$ é subespaço de V.*

Exemplo 4.1.6 *O conjunto das matrizes simétricas, matrizes que são iguais à sua transposta, é um subespaço vetorial de $M_n(\mathbb{R})$.*

Exemplo 4.1.7 *Se V é um espaço vetorial e $v \in V$, o conjunto dos vetores da forma av, com $a \in \mathbb{R}$, é um subespaço de V.*

Exemplo 4.1.8 *O espaço das funções polinomiais sobre o corpo F é um subespaço do espaço de todas as funções de F em F.*

Definição 4.1.9 *Sejam V um espaço vetorial sobre um corpo F e W um subespaço de V. Chamamos de* **suplementar** *de W o subespaço W' de V tal que $V = W \oplus W'$.*

Observação 4.1.10 *Em geral existem muitos subespaços W' que são suplementares de W.*

Exemplo 4.1.11 *Sejam $V = \mathbb{R}^2$ um espaço vetorial (a coordenada real do plano) e $W = \{(x_1, x_2) \in \mathbb{R}^2, tal\ que\ x_2 = 0\}$ um subespaço de V (o eixo horizontal). Cada complemento de W é uma linha partindo da origem, sendo esta linha diferente do eixo horizontal.*

Se V não possui nenhuma estrutura além a de espaço vetorial, não existe uma maneira natural de escolher um dentre a variedade de suplementos de W. Contudo, há uma construção natural que associa a V e W um novo espaço vetorial que desempenha o papel do suplementar de W. A partir de agora passaremos a estudar esse novo espaço vetorial.

4.2 Espaços Quocientes

Agora que já sabemos o que é um subespaço vetorial e o suplementar de um subespaço, podemos iniciar nossos estudos sobre Espaços Quocientes. O espaço quociente é o novo espaço vetorial citado anteriormente que desempenhara o papel de suplementar de um subespaço W de V.

É importante ressaltar que esse espaço quociente não é um subespaço de V, portanto não pode ser realmente um subespaço suplementar de W. No entanto, ele é um espaço vetorial definido em termos de V e W que é isomorfo a todo subespaço W' suplementar de W.

4.2.1 Conceito de Espaço Quociente

Assim como fizemos em Grupos e Anéis, definiremos agora uma relação de equivalência determinada pelo subespaço W sobre o espaço vetorial V.

Definição 4.2.1 *Sejam V um espaço vetorial e W um subespaço de V. Para todo $\alpha, \beta \in V$, podemos estabelecer a seguinte relação:*

$$\alpha \sim \beta \Leftrightarrow \alpha - \beta \in W.$$

Quando isso acontece dizemos que α é **congruente** *à β* **módulo** *W e, escrevemos*

$$\alpha \equiv \beta, \, mod \, W.$$

A relação acima é de fato de uma relação de equivalência em V, já que

- $\alpha \equiv \alpha$, mod W, pois $\alpha - \alpha = 0 \in W$.
- Se $\alpha \equiv \beta$, mod W, então $\beta \equiv \alpha$, mod W. De fato, como W é subespaço de V, o vetor $(\alpha - \beta)$ está em W se, e somente se $(\beta - \alpha)$ está em W.
- Se $\alpha \equiv \beta$, mod W, e $\beta \equiv \gamma$, mod W, então $\alpha \equiv \gamma$, mod W. De fato, se $(\alpha - \beta)$ e $(\beta - \gamma)$ estão em W, então $(\alpha - \beta) + (\beta - \gamma) \in W \Rightarrow (\alpha - \gamma) \in W$.

Definição 4.2.2 *Sejam W um subespaço num espaço vetorial V e α um elemento de V. Definimos a* **classe lateral** *do vetor α como sendo o conjunto*

$$\alpha + W = \{\alpha + w; \ w \in W\}$$

Exemplo 4.2.3 *Retomando o exemplo 4.1.11, as classes laterais de W são as linhas horizontais.*

Exemplo 4.2.4 *Sejam o espaço vetorial $V = \mathbb{R}^2$ e W um subespaço unidimensional de V. Se imaginarmos V como sendo o plano euclidiano, W será uma reta passando pela origem. Se $\alpha = (x_1, x_2)$ é um vetor em V, a classe lateral $\alpha + W$ é a reta que passa pelo ponto (x_1, x_2) e é paralela à W.*

Observação 4.2.5 *É importante obeservar que uma mesma classe lateral pode surgir a partir de dois vetores diferentes, ou seja, se $\alpha \neq \beta$ é possível que $\alpha + W = \beta + W$.*

Observação 4.2.6 *Faz sentido falar de uma classe lateral H de W, sem especificar de que elemento, ou elementos, a classe H vem. Dizer que H é uma classe lateral de W significa simplesmente que há pelo menos um vetor α tal que $H = \alpha + W$.*

Definição 4.2.7 *O conjunto de todas as classes laterais de W será indicada por V/W, assim temos*

$$V/W = \{\alpha + W;\ \ \alpha \in V\}$$

A seguir, veremos que é possível definir a adção de vetores e a multiplicão escalar sobre V/W.

Adição em $\mathbf{V/W}$

A expressão a seguir define a adição de vetores em V/W

$$(\alpha + W) + (\beta + W) = (\alpha + \beta) + W,\ \forall\ \alpha,\ \beta \in V.$$

Muitos vetores distintos em V terão a mesma classe lateral em relação a W. Dessa forma, assim como fizemos com as classes G/H *e* A/I nos capítulos anteriores, vejamos que essa operação está bem definida, ou seja, que não depende das classes laterais envolvidas.

Se $\alpha \equiv \alpha'$, mod W, e $\beta \equiv \beta'$, mod W, então $(\alpha - \alpha') \in W$ e $(\beta - \beta') \in W$. Assim, existem $x_1, x_2 \in W$, tais que $\alpha = \alpha' + x_1$ e $\beta = \beta' + x_2$. Assim, temos

$$\begin{aligned}
(\alpha + W) + (\beta + W) &= (\alpha + \beta) + W \\
&= ((\alpha' + x_1) + (\beta' + x_2)) + W \\
&= ((\alpha' + \beta') + (x_1 + x_2)) + W \\
&= (\alpha' + \beta') + W + (x_1 + x_2) + W \\
&= (\alpha' + \beta') + W \\
&= (\alpha' + W) + (\beta' + W) \\
&= (\alpha + W) + (\beta + W).
\end{aligned}$$

Sejam $(\alpha + W),\ (\beta + W),\ (\gamma + W) \in {}^{V}\!/\!_{W}$. Verifiquemos que a adição definida em ${}^{V}\!/\!_{W}$ obedece as seguintes condições:

- **(Comutatividade)** $(\alpha+W)+(\beta+W) = (\alpha+\beta)+W = (\beta+\alpha)+W = (\beta+W)+(\alpha+W)$.
- **(Associatividade)** $(\alpha + W) + [(\beta + W) + (\gamma + W)] = (\alpha + W) + [(\beta + \gamma) + W] = [\alpha+(\beta+\gamma)]+W = [(\alpha+\beta)+\gamma]+W = [(\alpha+\beta)+W]+(\gamma+W) = [(\alpha+W)+(\beta+W)]+(\gamma+W)$.
- **(Elemento Neutro)** O elemento neutro das classes em ${}^{V}\!/\!_{W}$ é $0 + W = W$, ou seja, o próprio W.
- **(Oposto)** Para cada classe $\alpha+W$ existe a classe $(-\alpha)+W$, tal que essa classe é o oposto de $\alpha + W$. Vejamos que $(\alpha + W) + (-\alpha + W) = (\alpha - \alpha) + W = 0 + W = W$.

Multiplicação por escalar em ${}^{\mathbf{V}}\!/\!_{\mathbf{W}}$

A expressão a seguir define a multiplicação por escalar sobre ${}^{V}\!/\!_{W}$

$$c(\alpha + W) = (c\alpha) + W,\ \forall\ \alpha \in V\ e\ c \in F.$$

Vejamos que a mutiplicação escalar também está bem definida. Assim como fizemos na adição de vetores, consideremos $\alpha + W = \alpha' + W$. Desse modo:

$$\alpha + W = \alpha' + W \Rightarrow (\alpha - \alpha') \in W$$

Como W é subespaço vetorial, $\forall\ c \in F$ tem-se $c(\alpha - \alpha') \in W$, o que implica que:

$$\begin{aligned} c(\alpha - \alpha') + W &= 0 + W \quad \Rightarrow \\ (c\alpha - c\alpha') + W &= 0 + W \quad \Rightarrow \\ c\alpha + W &= c\alpha' + W \end{aligned}$$

Sejam $(\alpha+W),\ (\beta+W) \in {}^{V}\!/\!_{W}\ e\ c_1, c_2 \in F$. Verifiquemos que a multiplicação definida em ${}^{V}\!/\!_{W}$ obedece as seguintes condições:

- **(Associatividade)** $(c_1c_2)(\alpha + W) = [(c_1c_2)\alpha + W] = [c_1(c_2\alpha) + W] = c_1(c_2\alpha + W)$.
- **(Distributividade)** $c_1[(\alpha + W) + (\beta + W)] = c_1[(\alpha + \beta) + W] = c_1(\alpha + \beta) + W = [(c_1\alpha) + (c_1\beta)] + W = (c_1\alpha + W) + (c_1\beta + W) = c_1(\alpha + W) + c_1(\beta + W)$.

- **(Distributividade)** $(c_1 + c_2)(\alpha + W) = [(c_1 + c_2)\alpha] + W = [(c_1\alpha) + (c_2\alpha)] + W = (c_1\alpha) + W + (c_2\alpha) + W = c_1(\alpha + W) + c_2(\alpha + W)$.

Portanto, como o conjunto V/W obedece todos os axiomas que definem um espaço vetorial, podemos concluir que esse conjunto, munido das operações definidas acima, é um espaço vetorial.

Observação 4.2.8 *Sejam o escalar* $1 \in F$ *e* $\alpha + W \in V/W$. *Então,* $1(\alpha + W) = (1\alpha) + W = \alpha + W$.

Definição 4.2.9 *Sejam* V *um espaço vetorial sobre um corpo* F *e* W *um subespaço de* V. *O espaço vetorial* V/W, *introduzido pelas considerações acima, é chamado de* **espaço quociente**.

Vejamos um exemplo de espaço quociente.

Exemplo 4.2.10 *Sejam* $V = \mathbb{R}^5 = \{(x_1, x_2, x_3, x_4, x_5);\ x_i \in \mathbb{R}\}$ *um espaço vetorial sobre* F *e* $W = \{(x,\ y,\ z,\ r,\ s);\ x = y = z = r = 0\}$ *um subespaço vetorial de* V. *O conjunto* $\mathbb{R}^5/W$ *é um espaço quociente.*

Verifiquemos a seguir que o conjunto $\mathbb{R}^5/W$ é realmente um espaço quociente. Pela definição 4.2.7, temos que $\mathbb{R}^5/W = \{\alpha + W;\ \alpha \in \mathbb{R}^5\}$. Sejam $\alpha + W,\ \beta + W \in \mathbb{R}^5/W$ e $c \in F$, sabemos que

$$(\alpha + W) + (\beta + W) = (\alpha + \beta) + W \text{ e } c(\alpha + W) = (c\alpha) + W.$$

Sejam $\alpha = (x_1,\ x_2,\ x_3,\ x_4,\ x_5)$, $\beta = (x_6,\ x_7,\ x_8,\ x_9,\ x_{10})$ e $\gamma = (x_{11},\ x_{12},\ x_{13},\ x_{14},\ x_{15})$ e $c_1, c_2 \in F$, verifiquemos que a adição em $\mathbb{R}_5/W$ satisfaz as seguintes propriedades:

- **(Comutatividade)** $(\alpha + W) + (\beta + W) = (\alpha + \beta) + W = ((x_1,\ x_2,\ x_3,\ x_4,\ x_5) + (x_6,\ x_7,\ x_8,\ x_9,\ x_{10})) + W = (x_1 + x_6,\ x_2 + x_7,\ x_3 + x_8,\ x_4 + x_9,\ x_5 + x_{10}) + W = (x_6 + x_1,\ x_7 + x_2,\ x_8 + x_3,\ x_9 + x_4,\ x_{10} + x_5) + W = ((x_6,\ x_7,\ x_8,\ x_9,\ x_{10}) + ((x_1,\ x_2,\ x_3,\ x_4,\ x_5)) + W = (\beta + \alpha) + W = (\beta + W) + (\alpha + W)$.

- **(Associatividade)** $(\alpha + W) + ((\beta + W) + (\gamma + W)) = (\alpha + W) + ((\beta + \gamma) + W) = (\alpha + (\beta + \gamma)) + W = ((x_1,\ x_2,\ x_3,\ x_4,\ x_5) + ((x_6,\ x_7,\ x_8,\ x_9,\ x_{10}) + (x_{11},\ x_{12},\ x_{13},\ x_{14},\ x_{15}))) + W = ((x_1,\ x_2,\ x_3,\ x_4,\ x_5) + (x_6 + x_{11},\ x_7 + x_{12},\ x_8 + x_{13},\ x_9 + x_{14},\ x_{10} + x_{15})) + W = (x_1 + x_6 + x_{11},\ x_2 + x_7 + x_{12},\ x_3 + x_8 + x_{13},\ x_4 + x_9 + x_{14},\ x_5 + x_{10} + x_{15})) + W = ((x_1 + x_6,\ x_2 + x_7,\ x_3 + x_8,\ x_4 + x_9,\ x_5 + x_{10}) + (x_{11},\ x_{12},\ x_{13},\ x_{14},\ x_{15})) + W = (((x_1,\ x_2,\ x_3,\ x_4,\ x_5) + (x_6,\ x_7,\ x_8,\ x_9,\ x_{10})) + (x_{11},\ x_{12},\ x_{13},\ x_{14},\ x_{15})) + W = ((\alpha + \beta) + \gamma) + W = ((\alpha + \beta) + W) + (\gamma + W) = ((\alpha + W) + (\beta + W)) + (\gamma + W)$.

- **(Elemento Neutro)** Como já definimos, o elemento neutro das classes em V/W é o próprio W. De fato, $\forall\ (a+W) \in V/W,\ (a+W)+W = (a+W)+(0+W) = (a+0)+W = a+W$.

- **(Oposto)** Para cada classe $\alpha + W$ existe a classe $(-\alpha)+W$ que é o oposto da classe $\alpha + W$. Vejamos que $(\alpha+W)+(-\alpha+W) = (\alpha+(-\alpha))+W = ((x_1,\ x_2,\ x_3,\ x_4,\ x_5)+(-x_1,\ -x_2,\ -x_3,\ -x_4,\ -x_5))+W = (x_1-x_1,\ x_2-x_2,\ x_3-x_3,\ x_4-x_4,\ x_5-x_5)+W = (0,0,0,0,0)+W = 0+W = W$.

Verifiquemos agora que a multiplicação por escalar em $\mathbb{R}_5/W$ satisfaz as seguintes propriedades:

- **(Associatividade)** $(c_1c_2)(\alpha+W) = ((c_1c_2)\alpha)+W = ((c_1c_2)(x_1,\ x_2,\ x_3,\ x_4,\ x_5))+W = ((c_1c_2)x_1,\ (c_1c_2)x_2,\ (c_1c_2)x_3,\ (c_1c_2)x_4,\ (c_1c_2)x_5)+W = (c_1(c_2x_1),\ c_1(c_2x_2),\ c_1(c_2x_3),\ c_1(c_2x_4),\ c_1(c_2x_5))+W = c_1((c_2x_1,\ c_2x_2,\ c_2x_3,\ c_2x_4,\ c_2x_5)+W) = c_1(c_2(x_1,\ x_2,\ x_3,\ x_4,\ x_5)+W) = c_1(c_2(\alpha+W))$.

- **(Elemento Neutro)** Vejamos que $1(\alpha)+W = (1\alpha)+W = (1(x_1,\ x_2,\ x_3,\ x_4,\ x_5))+W = (1x_1,\ 1x_2,\ 1x_3,\ 1x_4,\ 1x_5)+W = (x_1,\ x_2,\ x_3,\ x_4,\ x_5)+W = \alpha+W$.

- **(Distributividade)** $c_1((\alpha+W)+(\beta+W)) = c_1((\alpha+\beta)+W) = (c_1(\alpha+\beta))+W = (c_1((x_1,\ x_2,\ x_3,\ x_4,\ x_5)+(x_6,\ x_7,\ x_8,\ x_9,\ x_{10})))+W = (c_1(x_1,\ x_2,\ x_3,\ x_4,\ x_5)+c_1(x_6,\ x_7,\ x_8,\ x_9,\ x_{10}))+W = (c_1(x_1,\ x_2,\ x_3,\ x_4,\ x_5)+W)+(c_1(x_6,\ x_7,\ x_8,\ x_9,\ x_{10})+W) = (c_1\alpha+W)+(c_1\beta+W) = c_1(\alpha+W)+c_1(\beta+W)$.

- **(Distributividade)** $(c_1+c_2)(\alpha+W) = ((c_1+c_2)\alpha)+W = ((c_1+c_2)(x_1,\ x_2,\ x_3,\ x_4,\ x_5))+W = ((c_1(x_1,\ x_2,\ x_3,\ x_4,\ x_5))+(c_2(x_1,\ x_2,\ x_3,\ x_4,\ x_5)))+W = (c_1\alpha+c_2\alpha)+W = ((c_1\alpha)+(c_2\alpha))+W = (c_1\alpha+W)+(c_2\alpha+W) = c_1(\alpha+W)+c_2(\alpha+W)$.

Logo, pela definição 4.2.15, como todas as propriedades que definem espaço vetorial são satisfeitas, temos que o conjunto das classes de equivalência $\mathbb{R}^5/W$ é um espaço quociente.

Definição 4.2.11 *Uma transformação linear natural Q de V sobre V/W, é definida por*

$$Q(\alpha) = \alpha + W.$$

Q é chamada de **transformação quociente** *ou* **aplicação quociente** *de V sobre V/W.*

Observação 4.2.12 *É importante ver que definimos as operações em* V/W *de forma que essa tranformação Q viesse a ser linear.*

Observação 4.2.13 *Notemos que o núcleo de Q é exatamente o subespaço W.*

Após estudarmos os espaços quocientes, podemos agora estabelecer a relação entre V/W e os subespaços de V que são suplementares de W, como haviamos mencionado no início dessa seção.

Teorema 4.2.14 *Seja W um subespaço do espaço vetorial V e seja Q a transformação quociente de V sobre* V/W. *Suponhamos que W' seja um subespaço de V. Então,* $V = W \oplus W'$ *se, e somente se, a restrição de Q à W' é um isomorfismo de W' em* V/W.

Em resumo, o que o teorema acima quer nos dizer é que W' é um suplementar de W se, e somente se, W' é um subespaço que contém um elemento de cada classe lateral de W. Ele mostra que quando $V = W \oplus W'$ a aplicação quociente Q identifica W' com V/W. Desse modo, temos que $(W \oplus W')/W$ é isomorfo a W' de uma maneira natural.

Podemos de maneira simples determinar a dimensão de um espaço quociente, como mostra o teorema a seguir.

Teorema 4.2.15 (Dimensão do Espaço Quociente) *Se W é um subespaço m-dimensional de V, e V é um espaço vetorial n-dimensional, então* V/W *tem dimensão n - m, ou seja,*

$$dim\left(V/W\right) = dim(V) - dim(W).$$

Exemplo 4.2.16 *Trazendo novamente o espaço quociente* $\mathbb{R}^5/W$, *visto no exemplo 4.2.10, verifiquemos que o mesmo possui dimensão 4. Não é difícil perceber que o espaço vetorial* $\mathbb{R}^5$ *sobre F tem dimensão 5. Claramente W é um subespaço vetorial de dimensão 1. Pelo Teorema 4.2.15*

$$dim\left(\mathbb{R}^5/W\right) = dim(\mathbb{R}^5) - dim(W) = 5 - 1 = 4.$$

Sejam $\alpha + W,\ \beta + W \in \mathbb{R}^5/W$, *sabemos que essas classes serão equivalentes se, e somente se,* $\alpha - \beta \in W$, *o que significa que as quatro primeiras coordenadas têm que ser iguais, ou seja, tem que ser nulas. Dessa forma, concluímos que nesse exemplo as quatro primeiras coordenadas que importam, e portanto, o espaço quociente* $\mathbb{R}^5/W$ *tem dimensão 4, assim como confirma o teorema.*

Vejamos mais um exemplo para entendermos melhor.

Exemplo 4.2.17 *Sejam o espaço vetorial* $\mathbb{R}^5$ *sobre* F *e o subespaço vetorial* $W = \{(x, y, z, r, s) \in \mathbb{R}^5;\ x = y = z = 0\}$. *Nesse caso,* W *possui dimensão 2. Assim como fizemos no exemplo anterior, sejam* $\gamma + W,\ \lambda + W \in \mathbb{R}^5/W$, *essas classes laterais serão equivalentes se, e somente se,* $\gamma - \lambda \in W$, *o que ocorrerá somente se as três primeiras coordenadas de* γ *e* λ *forem iguais. Sendo assim, as coordenadas que importam são as três primeiras, e portanto, o espaço quociente* $\mathbb{R}^5/W$ *tem dimensão 3. Pelo teorema 4.2.15*

$$dim\left(\mathbb{R}^5/W\right) = dim(\mathbb{R}^5) - dim(W) = 5 - 2 = 3.$$

É importante ressaltar que o espaço quociente em si não facilita tanto as coisas, como acontece nos anéis quocientes. No capítulo 3 vimos que o quociente em anéis reduz algo infinito em algo finito, o que pode ser muito prático. Em espaços vetoriais, como acabamos de ver, o quociente apenas reduz a dimensão. Vimos, por exemplo, que quocientando um espaço vetorial de dimensão 5 por um subespaço vetorial de dimensão 2 temos um espaço quociente de dimensão 3. No entanto, perceba que se precisarmos trabalhar com um espaço vetorial de dimensão 3 podemos contruí-lo de uma forma muito mais simples do que atraves do quociente.

Assim como fizemos em Grupos e Anéis Quocientes, a seguir traremos o Primeiro Teorema do Isomorfismo, que como será possível perceber, é semelhante em todas as estruturas estudadas até aqui.

Teorema 4.2.18 (Primeiro Teorema do Isomorfismo) *Sejam* V *e* Z *espaços vetoriais sobre o corpo* F *e* $\overline{T} : V \to Z$ *uma transformação linear. Então a aplicação*

$$T : V/Nuc(\overline{T}) \to Im(\overline{T}),\ \textit{definida por}\ T(\alpha + Nuc(\overline{T})) = \overline{T}(\alpha)$$

é um isomorfismo.

Demonstração: Chamaremos o núcleo de $\overline{T}$ de N. Assim, queremos mostrar que a transformação linear $T : V/N \to Im(\overline{T})$ é um isomorfismo.

Inicialmente mostraremos que T está bem definida. Para isso devemos verificar que, se $\alpha' \in \alpha + N$, então $T(\alpha + N) = T(\alpha' + N)$. Note que se $\alpha' \in \alpha + N$, então $\alpha' = \alpha + n$ para algum $n \in N$. Portanto:

- $T(\alpha' + N) = \overline{T}(\alpha') = \overline{T}(\alpha + n) = \overline{T}(\alpha) + \overline{T}(n) = \overline{T}(\alpha) + e' = \overline{T}(\alpha) = T(\alpha + N)$.

Agora, mostraremos que está aplicação é uma transformação linear:

- $T((\alpha+N)+(\beta+N)) = T((\alpha+\beta)+N) = \overline{T}(\alpha+\beta) = \overline{T}(\alpha)+\overline{T}(\beta) = T(\alpha+N)+T(\beta+N)$.
- $T(c(\alpha+N)) = T(c\alpha+N) = \overline{T}(c\alpha) = c\overline{T}(\alpha) = cT(\alpha+N)$.

Logo, T é uma transformação linear e resta mostrar que é também bijetora.

- $\overline{T}(\alpha) = \overline{T}(\alpha') \Rightarrow \overline{T}(\alpha) - \overline{T}(\alpha') = 0_Z \Rightarrow \overline{T}(\alpha-\alpha') = 0_Z \Rightarrow \alpha-\alpha' \in N \Rightarrow \alpha+N = \alpha'+N$. Logo, T é injetora.
- Seja $\beta \in Im(\overline{T})$, existe $\alpha \in V$, tal que $\beta = \overline{T}(\alpha)$. Considerando a classe de equivalência $\alpha+N \in {}^{V}\!/\!_{W}$, tem-se $T(\alpha+N) = \overline{T}(\alpha) = \beta$. Logo, T é sobrejetora.

Assim, como a aplicação T é uma tranformação linear bijetora, podemos concluir que T é um isomorfismo. ■

Neste capítulo estudamos a construção dos espaços quocientes. Inicialmente relembramos a definição de subespaços vetoriais e subespaços suplementares, definimos uma relação de equivalência entre os elementos de um espaço vetorial e em seguida definimos as classes laterais nesse conjunto, que se observarmos, é bastante semelhante ao que fizemos em anéis. Por fim, definimos o conjunto de todas as classes laterais ${}^{V}\!/\!_{W}$ e definimos as operações de adição de vetores e multiplicação por escalar nesse conjunto, operações essas que estão bem definidas e que obedecem as condições que definem um espaço vetorial. Logo, vimos que o conjunto quociente ${}^{V}\!/\!_{W}$ é também um espaço vetorial, o Espaço Quociente.

No próximo capítulo veremos como se dá a construção das álgebras quocientes, conteúdo pouco abordado nos livros, mas que desempenha um importante papel na teoria das álgebras com identidades polinomiais.

Capítulo 5

Álgebras Quocientes

Nesse capítulo estudaremos uma estrutura algébrica que geralmente não é trabalhada durante a graduação, a Álgebra. Veremos sua definição, algumas propriedades, exemplos e por fim a construção do quociente dessa estrutura, que por sua vez, se dá de forma muito semelhante às estruturas que vimos nos capítulos anteriores.

5.1 Definição de Álgebra

No Capítulo 1 vimos a definição de Anéis e Espaços Vetoriais. Essas definições serão muito importantes para que possamos entender o que são às Álgebras, e consequentemente a construção das Álgebras quocientes. Veremos também que as àlgebras obedecem propriedades semelhantes às estudadas na Teoria de Anéis e de Espaços Vetoriais.

Inicialmente, tomemos como exemplos os conjuntos $\mathbb{C}$ e $M_2(\mathbb{R})$ que, como vimos no Capítulo 1, obedecem as condições que definem anéis e espaços vetoriais simultaneamente. Esses são nossos primeiros exemplos de álgebras, mas sem mais delongas, vejamos a seguir a definição formal dessa estrutura.

Definição 5.1.1 *Um espaço vetorial R é chamado de uma álgebra (ou de uma $\mathbb{K}$-álgebra) se R é munido de uma operação binária $*$, chamada de multiplicação tal que, para todos $a,\ b,\ c \in R$ e $\alpha \in \mathbb{K}$ as seguintes condições são satisfeitas:*

1. $(a + b) * c = a * c + b * c$;
2. $a * (b + c) = a * b + a * c$;
3. $\alpha(a * b) = (\alpha a) * b = a * (\alpha b)$.

Vale ressaltar que a partir daqui estamos denotando a multiplicação por $*$ e a multiplicação por escalar por $\cdot$. No entanto, quando não houver possibilidade de confusão, denotaremos ambas por $\cdot$.

Como havia dito, essa é a definição mais formal encontrada nos livros. No entanto, tentaremos trazer aqui um definição mais simples, apenas para facilitar a compreensão do que vem a ser uma álgebra.

Definição 5.1.2 *Uma* **álgebra** *sobre um corpo $\mathbb{K}$ é um conjunto não vazio R munido de uma operação de adição (denotada por $+$), uma operação de multiplicação (denotada por $*$) e uma operação de multiplicação por escalar, entre os elementos de $\mathbb{K}$ e de R, tais que as seguintes condições são satisfeitas:*

1. *R é um anel, ou seja, em relação às operações de adição e multiplicação o conjunto R satisfaz as propriedades que definem anel (vistas em 1.2.1);*
2. *R é um espaço vetorial, ou seja, o conjunto R em relação as operações de adição e multiplicação por escalar satisfaz as propriedades vistas na definição 1.3.1;*
3. *$(\alpha \cdot a) * b = a * (\alpha \cdot b) = \alpha \cdot (a * b),\ \forall\ a,\ b \in R$ e $\alpha \in \mathbb{K}$.*

Vejamos alguns exemplos de álgebras.

Exemplo 5.1.3 *O conjunto dos números complexos $\mathbb{C}$ com as operações de adição, multiplicação e multiplicação por escalar usuais é uma álgebra, em específico, uma $\mathbb{R}$-álgebra.*

Observação 5.1.4 *Sabemos que a operação de multiplicação em $\mathbb{C}$ é comutativa, o que não ocorre com a multiplicação em $M_n(\mathbb{K})$. Nesse caso, dizemos que $\mathbb{C}$ é uma* **álgebra comutativa**.

Tomando $A, B \in M_2(\mathbb{R})$, tal que

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} e\ B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

Vemos que

$$A.B = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} . \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}.b_{11} + a_{12}.b_{21} & a_{11}.b_{12} + a_{12}.b_{22} \\ a_{21}.b_{11} + a_{22}.b_{21} & a_{21}.b_{12} + a_{22}.b_{22} \end{pmatrix}\ e$$

$$B.A = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} . \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} b_{11}.a_{11} + b_{12}.a_{21} & b_{11}.a_{12} + b_{12}.a_{22} \\ b_{21}.a_{11} + b_{22}.a_{21} & b_{21}.a_{12} + b_{22}.a_{22} \end{pmatrix},$$

ou seja, temos que $A.B \neq B.A$. Logo, o conjunto das matrizes $M_2(\mathbb{R})$ não é uma álgebra comutativa, assim como qualquer conjunto de matrizes de ordem n.

Exemplo 5.1.5 *O conjunto $\mathbb{K}[x]$ dos polinômios*

$$f(x) = c_0 + c_1 x + \cdots + c_k x^k$$

em que $c_i \in \mathbb{K}\ \forall\ i \in \{0, \ldots, k\}$ e k um inteiro não negativo é uma álgebra com a adição, multiplicação e multiplicação por escalar usuais de polinômios de uma variável.

Exemplo 5.1.6 *O conjunto dos polinômios comutativos nas variáveis x e y com coeficientes em $\mathbb{K}$ denotado por $\mathbb{K}[x, y]$ é uma álgebra. Um polinômio f desse tipo é da forma*

$$f(x, y) = c_{00} + c_{10}x + c_{01}y + c_{11}xy + \cdots + c_{kl}x^k y^l,$$

com $c_{ij} \in \mathbb{K},\ \forall\ i \in \{0, \ldots, k\},\ \forall\ j \in \{0, \ldots, l\}$ e k, l inteiros não negativos.

Exemplo 5.1.7 *O conjunto dos polinômios sobre o corpo $\mathbb{K}$, nas variáveis x e y, com a condição adicional de que $xy \neq yx$, ou seja, as variáveis não são comutativas, denotado por $\mathbb{K}\langle x\rangle$, munido da adição, multiplicação e multiplicação por escalar é uma álgebra.*

Exemplo 5.1.8 *Se $X = \{x_1, x_2, \ldots\}$ é um conjunto infinito, $\mathbb{K}\langle X\rangle$, munido das operações usuais, é uma álgebra, chamada de* **álgebra associativa livre***, livremente gerada por X.*

A seguir veremos algumas propriedades e conceitos de álgebra linear e de teoria de anéis que serão importantes para o estudo de álgebras que faremos posteriormente.

5.1.1 Algumas propriedades de Álgebras

Definição 5.1.9 *Seja V um espaço vetorial sobre um corpo $\mathbb{K}$. Uma* **base** *de V é um conjunto $B \subset V$ linearmente independente que gera V. Em outras palavras, isso significa que cada $v \in V$ pode ser escrito, de modo único, como uma combinação linear*

$$v = \alpha_1 b_1 + \alpha_2 b_2 + \cdots + \alpha_m b_m$$

de elementos da base $b_1, b_2, \ldots, b_m$ com elementos escalares $\alpha_1, \alpha_2, \ldots, \alpha_m$ do corpo $\mathbb{K}$.

Definição 5.1.10 *Dizemos que um espaço vetorial V tem dimensão finita se possui uma base finita, ou seja, $B = \{b_1, \ldots, b_k\}$ com um número finito k de elementos. Esse número k, que é o mesmo para todas as bases de V, chama-se dimensão do espaço vetorial V que é denotada como $dim_{\mathbb{K}} V = k$.*

Dizemos também que um espaço vetorial V tem dimensão infinita, e denotamos por $\dim_{\mathbb{K}} V = \infty$, quando ele não tem dimensão finita, ou seja, nenhum subconjunto finito de V é uma base de V.

Observação 5.1.11 *Quando falarmos da dimensão de uma álgebra R, estamos nos referindo a sua dimensão como espaço vetorial.*

Definição 5.1.12 *Dizemos que uma álgebra R é comutativa se for um anel comutativo, ou seja, para todo $a, b \in R$ temos que $a * b = b * a$.*

Definição 5.1.13 *Uma* **subálgebra** *de uma álgebra R é um subconjunto não vazio $S \subset R$ que é fechado em relação as três operações de R, ou seja, este subconjunto é simultaneamente um subanel e um subespaço vetorial de R.*

Vejamos a seguir que o conjunto das matrizes triangulares superiores $U_n(\mathbb{K})$, isto é, matrizes cujos elementos abaixo da diagonal principal são todos nulos, é uma subálgebra da álgebra $M_n(\mathbb{K})$ das matrizes $n \times n$. Como já vimos, uma álgebra é também um espaço vetorial, e consequentemente, uma subálgebra é também um subespaço vetorial. Desse modo, usaremos o Teorema 4.1.2 para demonstrar os próximos exemplos.

Exemplo 5.1.14 *O conjunto das matrizes triangulares $U_2(\mathbb{R})$ é uma subálgebra da álgebra $M_2(\mathbb{R})$. É fácil notar que quaisquer elementos de $U_2(\mathbb{R})$ pertencem à $M_2(\mathbb{R})$, ou seja, $U_2(\mathbb{R})$ é um subconjunto de $M_2(\mathbb{R})$. Desse modo, sejam A e $B \in U_2(\mathbb{R})$ e $\alpha \in \mathbb{R}$, tal que*

$$A = \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix} \text{ e } B = \begin{pmatrix} b_{11} & b_{12} \\ 0 & b_{22} \end{pmatrix}$$

queremos mostrar que $\alpha A + B \in U_2(\mathbb{R})$.

$$\alpha A + B = \alpha \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ 0 & b_{22} \end{pmatrix} = \begin{pmatrix} \alpha a_{11} & \alpha a_{12} \\ 0 & \alpha a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ 0 & b_{22} \end{pmatrix}$$

$$\alpha A + B = \begin{pmatrix} \alpha a_{11} + b_{11} & \alpha a_{12} + b_{12} \\ 0 & a_{22} + b_{22} \end{pmatrix} \in U_2(\mathbb{R}).$$

Portanto, pelo Teorema 4.1.2, concluímos que o conjunto das matrizes triangulares de ordem 2 são subálgebras das matrizes quadradas de ordem 2.

Exemplo 5.1.15 *O conjunto das matrizes triangulares $U_3(\mathbb{R})$ é subálgebra da álgebra $M_3(\mathbb{R})$. Dessa forma, sejam $C, D \in U_3(\mathbb{R})$ matrizes triangulares de ordem 3 e $\alpha \in \mathbb{R}$, tal que*

$$C = \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ 0 & c_{22} & c_{23} \\ 0 & 0 & c_{33} \end{pmatrix} \text{ e } D = \begin{pmatrix} d_{11} & d_{12} & d_{13} \\ 0 & d_{22} & d_{23} \\ 0 & 0 & d_{33} \end{pmatrix}$$

assim como fizemos no exemplo anterior, queremos mostrar que $\alpha C + D \in U_3(\mathbb{R})$.

$$\alpha C + D = \alpha \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ 0 & c_{22} & c_{23} \\ 0 & 0 & c_{33} \end{pmatrix} + \begin{pmatrix} d_{11} & d_{12} & d_{13} \\ 0 & d_{22} & d_{23} \\ 0 & 0 & d_{33} \end{pmatrix} = \begin{pmatrix} \alpha c_{11} & \alpha c_{12} & \alpha c_{13} \\ 0 & \alpha c_{22} & \alpha c_{23} \\ 0 & 0 & \alpha c_{33} \end{pmatrix} + \begin{pmatrix} d_{11} & d_{12} & d_{13} \\ 0 & d_{22} & d_{23} \\ 0 & 0 & d_{33} \end{pmatrix}$$

$$\alpha C + D = \begin{pmatrix} \alpha c_{11} + d_{11} & \alpha c_{12} + d_{12} & \alpha c_{13} + d_{13} \\ 0 & \alpha c_{22} + d_{22} & \alpha c_{23} + d_{23} \\ 0 & 0 & \alpha c_{33} + d_{33} \end{pmatrix} \in U_3(\mathbb{R})$$

Portanto, novamente pelo Teorema 4.1.2, concluímos que o conjunto das matrizes triangulares de ordem 3 são subálgebras das matrizes quadradas de ordem 3.

Observação 5.1.16 *O conjunto $\mathbb{K}[x]$ é uma subálgebra de $\mathbb{K}[x, y]$.*

Como o Teorema 4.1.2 é válido também para subálgebras, podemos reescrevê-lo voltado para as álgebras, e assim temos o teorema seguinte.

Teorema 5.1.17 *Seja R uma álgebra sobre um corpo $\mathbb{K}$ e $S \neq \emptyset$ um subconjunto de R, dizemos que S é uma subeálgebra em R se, e somente se, para cada $a,\ b \in R$ e cada escalar $\alpha \in \mathbb{K}$, $\alpha a + b \in S$.*

Definição 5.1.18 *Uma subálgebra I de R é chamada de ideal à esquerda de R se $RI \subset I$, ou seja, $ai \in I$ para todo $a \in R,\ i \in I$. De forma similar, é chamada de ideal à direita de*

R se $I.R \subset I$, ou seja, $ia \in I$ para todo $a \in R$, $i \in I$. Quando I é simultaneamente um ideal à direita e à esquerda, dizemos simplesmente que I é um ideal de R.

Definição 5.1.19 *Seja S um subconjunto qualquer de R, definimos o ideal gerado por S como o menor ideal de R que contém S. Este ideal é usualmente denotado por $\langle S \rangle$, se S é não vazio, sendo exatamente o conjunto de todas as somas finitas da forma*

$$a_1 s_1 c_1 + a_2 s_2 c_2 + \cdots + a_m s_m c_m$$

em que $a_i, c_i \in R$ e $s_i \in S$, para todo $i \in \{1, 2, \ldots, m\}$

Um ideal I é gerado por um subconjunto $S \subset I$ se $I = \langle S \rangle$. Além disso, se existe S tal que isso ocorra, dizemos que I é finitamente gerado.

Definiremos a seguir a ideia de homomorfismo no contexto de álgebras.

Definição 5.1.20 *Sejam R_1 e R_2 duas álgebras, dizemos que a função $\varphi : R_1 \longrightarrow R_2$ é um homomorfismo de álgebras se, para todo $a, b \in R_1$ e $\alpha \in \mathbb{K}$, temos:*

1. $\varphi(a + b) = \varphi(a) + \varphi(b)$;
2. $\varphi(a * b) = \varphi(a) * \varphi(b)$;
3. $\varphi(1_{R_1}) = 1_{R_2}$;
4. $\varphi(\alpha \cdot a) = \alpha \cdot \varphi(a)$.

Observação 5.1.21 *De forma similar a introdução de homomorfismos de álgebras acima, introduzimos a noção de isomorfismo, automorfismo e endomorfismo.*

5.2 Álgebras Quocientes

Finalmente, agora que já sabemos o que é uma álgebra, podemos falar sobre álgebras quocientes. Não será difícil perceber que a construção dessa estrutura se dá de forma semelhante ao que fizemos nos capítulos anteriores. Mais adiante veremos que o quociente das álgebras desempenha um papel importante na teoria de álgebras com identidades polinomiais, mas sem mais delongas, vejamos a seguir a definição de classe lateral na álgebra.

Definição 5.2.1 *Seja R uma álgebra e I um ideal em R. Para todo $a, b \in R$ podemos estabelecer a seguinte relação:*

$$a \sim b \Leftrightarrow a - b \in I$$

A relação acima trata-se uma relação de equivalência sobre R, pois:

1. $a \sim a$, pois $a - a = 0 \in I$;
2. Se $a \sim b \Rightarrow a - b \in I \Rightarrow -(a - b) \in I \Rightarrow b - a \in I \Rightarrow b \sim a$;
3. Se $a \sim b$ *e* $b \sim c \Rightarrow (a - b) \in I$ *e* $(b - c) \in I \Rightarrow (a - b) + (b - c) \in I \Rightarrow a - c \in I \Rightarrow a \sim c$.

Definição 5.2.2 *Sejam I um ideal numa álgebra R e $a \in R$, definimos a* **classe lateral à esquerda** *de a como sendo o conjunto*

$$a + I = \{a + i;\ i \in I\}.$$

Definição 5.2.3 *Denotamos o conjunto formado por todas as classes laterais à esquerda de I com relação à R, chamado de conjunto quociente, por*

$$R/I = \{a + I;\ a \in R\}.$$

A seguir veremos que podemos definir a adição, a multiplicação e a multiplicação por escalar no conjunto R/I.

Adição em $\mathbf{R/I}$

A expressão a seguir define a adição em R/I

$$(a + I) + (b + I) = (a + b) + I,\ \forall\ a,\ b \in R.$$

Assim como fizemos em grupos, anéis e espaços vetoriais, verifiquemos que essa operação está bem definida. Desse modo, se $a + I = a' + I$ *e* $b + I = b' + I$, então existem x_1 *e* $x_2 \in I$, tais que $a = a' + x_1$ *e* $b = b' + x_2$. Logo

$$\begin{aligned}
(a + I) + (b + I) &= (a + b) + I \\
&= ((a' + x_1) + (b' + x_2)) + I \\
&= ((a' + b') + (x_1 + x_2)) + I \\
&= (a' + b') + I + (x_1 + x_2) + I\ . \\
&= (a' + b') + I \\
&= (a' + I) + (b' + I) \\
&= (a + I) + (b + I).
\end{aligned}$$

Sejam $(a+I), (b+I)$ *e* $(c+I) \in R/I$. Verifiquemos, que a adição definida em R/I obedece as seguintes condições:

- **(Associatividade)** $(a+I)+((b+I)+(c+I)) = (a+I)+((b+c)+I) = (a+(b+c))+I = ((a+b)+c)+I = ((a+b)+I)+(c+I) = ((a+I)+(b+I))+(c+I)$.
- **(Elemento Neutro)** O elemento neutro das classes de equivalência é a classe $0+I = I$, ou seja, o próprio I. De fato, $\forall\ a+I \in {}^{R}\!/_{I},\ (a+I)+(0+I) = (a+0)+I = a+I$. De modo análogo provamos que $(0+I)+(a+I) = a+I$.
- **(Oposto)** Para a classe $a+I$ existe a classe $(-a)+I$, que é o seu oposto. De fato, $(a+I)+(-a+I) = (a-a)+I = 0+I = I$.
- **(Comutatividade)** $(a+I)+(b+I) = (a+b)+I = (b+a)+I = (b+I)+(a+I)$.

Multiplicação em ${}^{\mathbf{R}}\!/_{\mathbf{I}}$

A expressão a seguir define uma lei de composição interna em ${}^{R}\!/_{I}$.

$$(a+I).(b+I) = (a.b)+I,\ \forall\ a,\ b \in R.$$

Veremos que está operação também está bem definida. Assim como fizemos para a adição, consideremos que se $a+I = a'+I$ *e* $b+I = b'+I$, então existem x_1 *e* $x_2 \in I$, tais que $a = a'+x_1$ *e* $b = b'+x_2$.

$$\begin{aligned}
(a+I).(b+I) &= (a.b)+I \\
&= (a'+x_1)(b'+x_2)+I \\
&= (a'.b'+a'.x_2+x_1.b'+x_1.x_2)+I \\
&= (a'.b'+I)+((\underbrace{a'.x_2+x_1.b'+x_1.x_2}_{\in I})+I), pois \text{Ié ideal.} \\
&= a'.b'+I \\
&= (a'+I).(b'+I) \\
&= (a+I).(b+I).
\end{aligned}$$

Essa lei de composição é a multiplicação em ${}^{R}\!/_{I}$ e apresenta as seguintes propriedades:

- **(Associatividade)** $(a+I).((b+I).(c+I)) = (a+I).(b.c+I) = a.(b.c)+I = (a.b).c+I = (a.b+I).(c+I) = ((a+I).(b+I)).(c+I)$
- **(Distributividade)** $(a+I)\cdot[(b+I)+(c+I)] = (a+I)\cdot[(b+c)+I] = a\cdot(b+c)+I = (a\cdot b+a\cdot c)+I = (a\cdot b+I)+(a\cdot c+I) = (a+I)\cdot(b+I)+(a+I)\cdot(c+I)$.

Não é difícil perceber que em relação as operações de adição e multiplicação o conjunto $^{R}/_{I}$, assim como o conjunto quociente $^{A}/_{I}$ visto no Capítulo 3, é também um anel. A seguir, veremos mais uma operação que está definida dentro desse conjunto.

Multiplicação por escalar em $^{\mathbf{R}}/_{\mathbf{I}}$

A expressão a seguir define a multiplicação por escalar em $^{R}/_{I}$.

$$c(a+I) = (ca) + I, \ \forall \ a \in I \ e \ c \in F.$$

Vejamos que está operação também está bem definida. Considerando $a + I = a' + I$, assim como fizemos nas operações anteriores, temos que:

$$a + I = a' + I \Rightarrow (a - a') \in I.$$

Para todo escalar $c \in F$ tem-se $c(a - a') \in I$, o que implica que:

$$\begin{aligned} c(a-a') + I &= 0 + I \quad \Rightarrow \\ (ca - ca') + I &= 0 + I \quad \Rightarrow \\ ca + I &= ca' + I \quad \Rightarrow \\ c(a+I) &= c(a'+I). \end{aligned}$$

Sejam $(a + I), \ (b + I) \in {}^{R}/_{I}$ e $c_1, \ c_2 \in F$, vejamos que a multiplicação por escalar definida em $^{R}/_{I}$ odece as seguintes propriedades:

- **(Associatividade)** $(c_1c_2)(a + I) = ((c_1c_2)a) + I = (c_1(c_2a)) + I = (c_1 + I)(c_2a + I)$.
- **(Distributividade)** $c_1((a+I)+(b+I)) = c_1((a+b)+I) = (c_1(a+b))+I = (c_1a+c_1b)+I = (c_1a + I) + (c_1b + I) = c_1(a + I) + c_1(b + I)$.
- **(Distributividade)** $(c_1 + c_2)(a + I) = ((c_1 + c_2)a) + I = ((c_1a) + (c_2a)) + I = (c_1a + I) + (c_2a + I) = c_1(a + I) + c_2(a + I)$.

Como acabamos de ver, o conjunto $^{R}/_{I}$ é munido também da operação de multiplicação por escalar. Sendo assim, o conjunto $^{R}/_{I}$ é também um espaço vetorial, visto que obedece os axiomas que definem um espaço vetorial. Portanto, pela definição 5.1.2 o conjunto das classes laterais $^{R}/_{I}$ é um álgebra.

Observação 5.2.4 *Sejam o escalar* $1 \in F$ *e* $a + I \in {}^{R}/_{I}$, *então* $1(a + I) = (1a) + I = a + I$.

Definição 5.2.5 *Sejam R uma álgebra sobre um corpo $\mathbb{K}$ e I uma subálgebra ideal em R. A álgebra ${}^{R}\!/_{I}$, introduzida pelas considerações acima, é chamada de* **álgebra quociente**.

Teorema 5.2.6 (Primeiro Teorema do Isomorfismo) *Sejam R e S álgebras e $\bar{\varphi} : R \to S$ um homomorfismo de álgebras. Então a aplicação*

$$\varphi : {}^{R}\!/_{Nuc(\bar{\varphi})} \to Im(\bar{\varphi}),\ \textit{definida por}\ \varphi(a + Nuc(\bar{\varphi})) = \bar{\varphi}(a)$$

é um isomorfismo de álgebras. Dessa forma

$${}^{R}\!/_{Nuc(\bar{\varphi})} \cong Im(\bar{\varphi}).$$

A demonstração desse teorema segue de forma análoga à demonstração do Primeiro Teorema do Isomorfismo para anéis na página 31.

Neste capítulo estudamos a contrução das álgebras quocientes, começando pela definição de álgebra, algumas propriedades e exemplos. Por se tratar de uma estrutura que é ao mesmo tempo um anel e um espaço vetorial, a construção das álgebras quocientes ocorre de forma muito semelhante ao que fizemos para anéis e espaços quocientes nos Capítulos 3 e 4. Inicialmente definimos uma relação de equivalência entre os elementos de uma álgebra, definimos classes laterais e o conjunto formado por todas as classes laterais de um ideal I sobre uma álgebra R. Por fim, mostramos que esse conjunto é munido das operações de adição, multiplicação e multiplicação por escalar, operações essas que estão bem definidas e que obedecem às condições que definem uma álgebra. Logo, vimos que o conjunto quociente ${}^{R}\!/_{I}$ é também uma álgebra, a Álgebra Quociente.

No próximo capítulo, estudaremos um pouco sobre as álgebras com identidades polinomiais, T-ideais e graduações.

Capítulo 6

Álgebras com Identidades Polinomiais

Chegamos ao capítulo final deste trabalho. No Capítulo 5 estudamos um pouco sobre álgebras e álgebras quocientes. Nesse capítulo falaremos sobre álgebras com identidades polinomiais, as PI-álgebras, T-ideais, e álgebras graduadas. Ao final desse capítulo veremos um exemplo concreto de álgebra quociente que desempenha um papel importante dentro da Teoria de Álgebras com Identidades Polinomiais.

6.1 PI-álgebra

Nessa seção estudaremos um pouco sobre álgebras com identidades polinomiais. Nas próximas seções veremos o que são os T-ideais e Identidades polinomiais graduadas.

Definição 6.1.1 *Seja $f(x_1, x_2, \ldots, x_n) \in \mathbb{K}\langle X\rangle$ e seja R uma álgebra. Dizemos que $f(x_1, x_2, \ldots, x_n)$ é uma* **identidade polinomial** *de R se*

$$f(a_1, a_2, \ldots, a_n) = 0 \text{ para todo } a_1, a_2, \ldots, a_n \in R.$$

Definição 6.1.2 *Se uma álgebra R satisfaz alguma identidade polinomial, dizemos que R é uma álgebra com identidades polinomiais, ou simplesmente uma* **PI-álgebra** *. O polinômio identicamente nula é chamado de identidade polinomial trivial.*

A seguir veremos alguns exemplos de álgebras com identidades polinomiais.

Exemplo 6.1.3 *Seja R uma álgebra comutativa, então $f(x_1, x_2) = x_1x_2 - x_2x_1$ é uma identidade polinomial de R.*

Exemplo 6.1.4 *A álgebra $M_2(\mathbb{K})$ satisfaz a identidade*

$$f(x_1, x_2, x_3) = [[x_1, x_2]^2, x_3] = (x_1x_2 - x_2x_1)^2x_3 - x_3(x_1x_2 - x_2x_1)^2,$$

conhecida como **identidade de Hall**. *Logo, $M_2(\mathbb{K})$ é uma álgebra com identidade polinomial.*

Definição 6.1.5 *O* **polinômio standard** *de grau m é dado por:*

$$s_m(x_1,\ x_2, \cdots, x_m) = \sum_{\sigma \in S_m} (sinal\sigma) x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(m)}.$$

Exemplo 6.1.6 *A álgebra $M_2(\mathbb{K})$ também satisfaz a identidade polinomial*

$$s_4(x_1, x_2, x_3, x_4) = 0,$$

conhecida como identidade standard de grau 4.

Exemplo 6.1.7 *A álgebra $U_n(\mathbb{K})$, das matrizes triangulares superiores, satisfaz a identidade*

$$[x_1, x_2] \dots [x_{2n-1}, x_{2n}]$$

A seguir veremos algumas definições fundamentais para entendermos os próximos exemplos.

Definição 6.1.8 *Dizemos que uma álgebra R é uma* **nil álgebra** *se para cada $a \in R$ existe um número $n \in \mathbb{N}$ tal que $a^n = 0$. Esse número n é chamado de índice de nilpotência do elemento a.*

Definição 6.1.9 *Dizemos que uma álgebra R é* **nilpotente** *se existe um número $n \in \mathbb{N}$ fixo, tal que o produto de quaisquer n elementos de R seja igual a zero. O menor número n com essa propriedade é chamado de índice de nilpotência da álgebra R.*

Exemplo 6.1.10 *Toda nil álgebra de índice limitado n é uma álgebra com identidades polinomiais, pois satisfaz a identidade $f(x_1) = x_1^n$.*

Exemplo 6.1.11 *Toda álgebra associativa nilpotente de classe $n-1$ é uma álgebra com identidades polinomiais, pois satisfaz a identidade $f(x_1, x_2, \dots, x_n) = x_1x_2 \dots x_n$.*

Agora que já vimos alguns exemplos de PI - álgebras, é natural que vejamos pelo menos um exemplo de uma álgebra que não é PI - álgebra.

Exemplo 6.1.12 *A álgebra $\mathbb{K}\langle X\rangle$ não é uma PI-álgebra.*
Demonstração: *Suponhamos por absurdo que $f(x_1, \dots, x_n)$ seja uma identidade polinomial não-nula de $\mathbb{K}\langle X\rangle$. Logo, $f(x_1, \dots, x_n) = f(f_1(x_1), \dots, f_n(x_n)) = 0$ onde $f_i(x_i) = x_i$ para $1 \leq i \leq n$, o que é absurdo, pois $f(x_1, \dots, x_n) \neq 0$.*

■

6.2 T - ideal

Seja R uma álgebra. O conjunto de todas as identidades polinomiais de R é denotado por $T(R)$, ou seja, $T(R) = \{f \in \mathbb{K}\langle X\rangle \mid f \text{ é uma identidade polinomial de } R\}$.

Teorema 6.2.1 *Seja R uma álgebra, o conjunto $T(R)$ é um ideal de $\mathbb{K}\langle X\rangle$. Além disso, ele possui a propriedade de ser invariante por endomorfismos de $\mathbb{K}\langle X\rangle$.*

Observação 6.2.2 *Dizer que $T(R)$ é invariante por endomorfismo de $\mathbb{K}\langle X\rangle$ significa dizer que para todo $f(x_1, \ldots, x_r) \in T(R)$, podemos trocar qualquer x_i, $i = 1, \ldots, r$, por qualquer elemento de $\mathbb{K}\langle X\rangle$ e f continuará sendo identidade polinomial de R.*

Definição 6.2.3 *Dada uma álgebra R, chamamos $T(R)$ de* **T-ideal** *de R.*

Exemplo 6.2.4 *Dos exemplos 6.1.4 e 6.1.6 da seção anterior temos que $[[x_1, x_2]^2, x_3]$ e s_4 estão no T- ideal $T(M_2(\mathbb{K}))$.*

A seguir, veremos a definição de base de um T-ideal. É importante destacar que a base da qual falaremos é diferente da base que estudamos em álgebra linear.

A interseção de uma família de T-ideais é também um T-ideal. Dessa forma, dado um subconjunto $S \subseteq \mathbb{K}\langle X\rangle$, podemos definir o T-ideal gerado por S, denotado por $\langle S\rangle^T$, como sendo a interseção de todos os T-ideais de $\mathbb{K}\langle X\rangle$ que contêm S.

Definição 6.2.5 *Se $S \subseteq T(R)$, tal que $\langle S\rangle^T = T(R)$, dizemos que S é uma* **base das identidades** *da álgebra R.*

A seguir, veremos alguns exemplos de bases das identidades para algumas álgebras.

Exemplo 6.2.6 *Se $\mathbb{K}$ é um corpo de característica zero, então uma base do T-ideal $T(M_2(\mathbb{K}))$ é dada por*

$$\{s_4(x_1, x_2, x_3, x_4), h_5(x_1, x_2, x_3)\}$$

onde, h_5 é uma identidade de Hall, de modo que $h_5(x_1, x_2, x_3) = [[x_1, x_2]^2, x_3]$.

Exemplo 6.2.7 *Se $\mathbb{K}$ é um corpo infinito de característica maior que 3, então uma base de $T(M_2(\mathbb{K}))$ é dada por*

$$\{s_4(x_1, x_2, x_3, x_4), [[x_1, x_2] \circ [x_3, x_4], x_5\}$$

em que $a \circ b = 1/2(ab + ba)$.

Já quando $\mathbb{K}$ é um corpo infinito de característica igual a 3, uma base para $T(M_2(\mathbb{K}))$ é

$$\{s_4(x_1,x_2,x_3,x_4),[[x_1,x_2]\circ[x_3,x_4],x_5],r_6(x_1,\dots x_6)\}$$

em que $r_6(x_1,\dots,x_6)=[x_1,x_2]\circ(u\circ v)-\frac{1}{8}([x_1,u,v,x_2]+[x_1,v,u,x_2]-[x_2,u,x_1,v]-[x_2,v,x_1,u])$ *com* $u=[x_3,x_4]$ *e* $v=[x_5,x_6]$.

Exemplo 6.2.8 *Seja* $\mathbb{K}$ *um corpo infinito, então*

$$\{[x_1,x_2][x_3,x_4]\dots[x_{2n-1},x_{2n}]\}$$

é uma base de $T(U_n(\mathbb{K}))$.

Definição 6.2.9 *A álgebra quociente* $\mathbb{K}\langle X\rangle/_I$ *será chamada de* **álgebra relativamente livre** *quando I for T-ideal das identidades polinomiais de alguma álgebra R.*

6.3 Identidades graduadas

Nessa seção falaremos um pouco sobre as identidades graduadas, estrutura adicional ao que fizemos na seção 6.1. As graduações nada mais são do que a quebra de álgebras em subespaços como soma direta bem comportada para a multiplicação.

Definição 6.3.1 *Seja* $(G,*)$ *um grupo. Uma álgebra R é dita* **G-graduada** *se temos uma família de subespaços* $\{R_g : g\in G\}$ *de R tal que*

$$R=\bigoplus_{g\in G}R_g$$

com $R_gR_h\subseteq R_{g*h}$*, para quaisquer* $g,h\in G$*, se G for grupo aditivo.*

Se G for grupo multiplicativo, podemos ainda definir $R=\bigoplus_{g\in G}R_g$*, com* $R_gR_h\subseteq R_{gh}$*, para quaisquer* $g,h\in G$.

Nessas condições, em qualquer um dos casos, dizemos que $R=\bigoplus_{g\in G}R_g$ *é uma* **G-graduação** *de R.*

Definição 6.3.2 *Os elementos* R_g *da definição anterior são chamados de* **elementos homogêneos de grau g**.

A seguir, veremos alguns exemplos de G-graduações.

Exemplo 6.3.3 *Qualquer álgebra R possui a seguinte G-graduação:* $R_0=R$ *e* $R_g=0$ *para todo* $g\in G-\{0\}$. *Essa graduação é chamada de* **graduação trivial** .

Exemplo 6.3.4 *Consideremos $R = M_2(\mathbb{K})$. É fácil ver que $M_2(\mathbb{K}) = R_0 \oplus R_1$, sendo $R_0 = \left\{ \begin{pmatrix} a_{11} & 0 \\ 0 & a_{22} \end{pmatrix}, a_{ij} \in \mathbb{K} \right\}$ e $R_1 = \left\{ \begin{pmatrix} 0 & a_{12} \\ a_{21} & 0 \end{pmatrix}, a_{ij} \in \mathbb{K} \right\}$ uma $\mathbb{Z}_2$-graduação de $M_2(\mathbb{K})$.*

Vejamos que o exemplo acima pode ser escrito de uma forma mais geral.

Exemplo 6.3.5 *Seja n um inteiro positivo e $R = M_n(\mathbb{K})$. Para todo $t \in \mathbb{Z}_n$, considere o subespaço $M_n(\mathbb{K})_t$ como subespaço gerado pelas matrizes $\{e_{ij}\}$ tais que $\overline{j-i} = t$. Assim, temos uma $\mathbb{Z}_n$-graduação de $M_n(\mathbb{K})$, dada por $R = \bigoplus_{t\in\mathbb{Z}_n} M_n(\mathbb{K})_t$. Chamamos essa graduação de* **$\mathbb{Z}_n$-graduação usual**.

Observação 6.3.6 *Na graduação do exemplo 6.3.4, as matrizes elementares são elementos homogêneos, onde $e_{11}, e_{22} \in R_0$ e $e_{12}, e_{21} \in R_1$. A partir daí temos a ideia que nos leva ao conceito de graduação elementar.*

Definição 6.3.7 *Seja R uma álgebra de matrizes G-graduada tal que todas as matrizes elementares são elementos homogêneos. Esta graduação é chamada de* **graduação elementar** *ou* **boa graduação** .

Vejamos alguns exemplos a seguir.

Exemplo 6.3.8 *Sejam $R = M_n(\mathbb{K})$ e $t \in \mathbb{Z}$, tal que*

$$M_n(\mathbb{K})_t = \begin{cases} \{0\} & , se\ |t| \geq n \\ \langle e_{ij} : j - i = t \rangle & , se\ |t| < n \end{cases} .$$

É fácil ver que $R = \bigoplus_{t\in\mathbb{Z}} M_n(\mathbb{K})_t$ defini uma $\mathbb{Z}$-graduação de $M_n(\mathbb{K})$, que será chamada de **$\mathbb{Z}$-graduação usual**.

Exemplo 6.3.9 *Do exemplo anterior, consideremos $n = 2$. Assim, para $R = M_2(\mathbb{K})$ temos a $\mathbb{Z}$-graduação usual dada por*

$$R_{-1} = \left\{ \begin{pmatrix} 0 & 0 \\ a_{21} & 0 \end{pmatrix} \right\},\ R_0 = \left\{ \begin{pmatrix} a_{11} & 0 \\ 0 & a_{22} \end{pmatrix} \right\},\ R_1 = \left\{ \begin{pmatrix} 0 & a_{12} \\ 0 & 0 \end{pmatrix} \right\}$$

com $a_{ij} \in \mathbb{K}$ para todo $i, j \in \{1, 2\}$.

Observe que no exemplo acima não usamos todos os elementos de $\mathbb{Z}$ como índices para os subespaços não nulos de R, como fizemos no exemplo 6.3.4. A partir daí, podemos introduzir o conceito de suporte de uma G-graduação.

Definição 6.3.10 *Seja R uma álgebra G-graduada. Chamamos de* **suporte** *da G-graduação de R o conjunto*

$$supp(R) = \{g \in G : R_g \neq 0\}.$$

Exemplo 6.3.11 *No exemplo 6.3.4 temos que $|supp(M_2(\mathbb{K}))| = 2$, em relação à $\mathbb{Z}_2$-graduação usual. Já no exemplo 6.3.9 temos que $|supp(M_2(\mathbb{K}))| = 3$, em relação à $\mathbb{Z}$-graduação usual.*

Exemplo 6.3.12 *Sejam $R = M_2(\mathbb{R})$ e $t \in \mathbb{Q}^*$, tal que*

$$R_t = \begin{cases} \{0\} & , se\ t \notin \{1, 2, 1/2\} \\ \langle e_{ij} : j/i = t \rangle & , se\ t \in \{1, 2, 1/2\} \end{cases}.$$

Dessa forma, temos

$$M_2(\mathbb{R}) = \begin{pmatrix} a_{11} & 0 \\ 0 & a_{22} \end{pmatrix} \oplus \begin{pmatrix} 0 & a_{12} \\ 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 \\ a_{21} & 0 \end{pmatrix} = R_1 \oplus R_2 \oplus R_{1/2}$$

com $a_{ij} \in \mathbb{R}$, para todo $i, j \in \{1, 2\}$. Logo, $|supp(M_2(\mathbb{R}))| = 2$, em relação à $\mathbb{Q}^*$- graduação.

Exemplo 6.3.13 *Consideremos em $R = M_2(\mathbb{K})$ a G-graduação dada por*

$$R_0 = \left\{ \begin{pmatrix} u & v \\ bv & u \end{pmatrix} : u, v \in \mathbb{K} \right\},\ R_g = \left\{ \begin{pmatrix} u & v \\ -bv & -u \end{pmatrix} : u, v \in \mathbb{K} \right\},\ R_h = 0$$

para todo $h \in G - \{0, g\}$ em que $g \in G$ é um elemento de ordem 2 e $b \in \mathbb{K} - \mathbb{K}^2$.

Dessa forma, temos que $|supp(M_2(\mathbb{K}))| = 2$. Vale ressaltar que como g tem ordem 2, temos $supp(M_2(\mathbb{K})) \simeq \mathbb{Z}_2$, neste caso. Logo, podemos dizer que está é uma $\mathbb{Z}_2$-graduação de $M_2(\mathbb{K})$.

Proposição 6.3.14 *Seja R uma álgebra G-graduada, então $1 \in R_1$.*

Definição 6.3.15 *Sejam R e S álgebras G-graduadas. Um homomorfismo $\varphi : R \to S$ é G-graduado se $\varphi(R_g) \subset \varphi(S_g)$ para todo $g \in G$.*

A seguir introduziremos a noção de álgebra associativa livre G-graduada, para posteriormente definirmos identidade polinomial G-graduada e T-ideal G-graduado.

Seja G um grupo, e para todo $g \in G$ consideremos um conjunto infinito enumerável X_g, tal que $X_{g_1} \bigcap X_{g_2} = \emptyset$, se $g_1 \neq g_2$. Sejam também $X = \bigcup_{g \in G} X_g$ e $\mathbb{K}\langle X \rangle$ uma álgebra

associativa livre com unidade. Definimos para $x_i \in X$, como $X = \bigcup X_g$, $\exists\ g \in G$ tal que $x_i \in X_g$. Definimos $\alpha(x_i) = g$, $\alpha(1) = 0$ e, para $x_1x_2\cdots x_n$,, tem-se que $\alpha(x_1x_2\cdots x_n) = \alpha(x_1) + \alpha(x_2) + \cdots + \alpha(x_n)$. Se m é um monômio de $\mathbb{K}\langle X\rangle$, então $\alpha(m)$ é o G-grau de m. Seja $\mathbb{K}\langle X\rangle_g$ o subespaço de $\mathbb{K}\langle X\rangle$ gerado pelos monômios de G-grau g. É fácil ver que $\mathbb{K}\langle X\rangle = \bigoplus_{g\in G}\mathbb{K}\langle X\rangle_g$, $\mathbb{K}\langle X\rangle_g\mathbb{K}\langle X\rangle_h = \mathbb{K}\langle X\rangle_{g+h}$ para todo $g, h \in G$, e $\mathbb{K}\langle X\rangle$ é uma álgebra G-graduada, chamada de **álgebra associativa livre G-graduada** .

Definição 6.3.16 *Seja $R = \bigoplus_{g\in G} R_g$ uma álgebra G-graduada e $f(x_1, x_2, \ldots, x_n) \in \mathbb{K}\langle X\rangle$. O polinômio $f(x_1, x_2, \ldots, x_n) \neq 0$ é uma* **identidade polinomial G-graduada**, *ou simplesmente uma identidade G-graduada de R se*

$$f(a_1, a_2, \ldots, a_n) = 0 \text{ para todo } a_1, a_2, \ldots, a_i \in R_{\alpha(x_i)}.$$

Definição 6.3.17 *Se uma álgebra G-graduada R satisfaz alguma identidade polinomial G-graduada, dizemos que R é uma* **PI-álgebra G-graduada**.

Definição 6.3.18 *Seja $\mathbb{K}\langle X\rangle$ uma álgebra associativa livre G-graduada. Um ideal I de $\mathbb{K}\langle X\rangle$ é um* **$\mathbf{T_G}$-ideal**, *ou um T-ideal G-graduado, se $\varphi(I) \subset I$ para todo endomorfismo G-graduado φ de $\mathbb{K}\langle X\rangle$. Em outras palavras, dizemos que I é um T_G-ideal se $f(g_1, g_2, \ldots, g_n) \in I$, para quaisquer $f(x_1, x_2, \ldots, x_n) \in I$ e $g_i \in \mathbb{K}\langle X\rangle_{\alpha(x_i)}$ com $i = 1, 2, \ldots, n$.*

Observação 6.3.19 *A noção de T_G-ideal gerado por um subconjunto S de $\mathbb{K}\langle X\rangle$ é análoga à ideia de T-ideal gerado por S. Sendo assim, denotaremos por $\langle S\rangle^{T_G}$ o T_G-ideal gerado por S.*

A seguir veremos um exemplo no qual é aplicada a álgebra quociente e diversos conceitos trabalhados ao longo dos capítulos 5 e 6. O exemplo trata-se de uma proposição da teoria de álgebras com identidades polinomiais que é fundamental na busca por geradores de T-ideais da álgebra de matrizes $M_2(\mathbb{K})$, pois facilita as contas e nos permite encontrar tais geradores.

Antes de enunciarmos a proposição, denotemos por I o $T_{\mathbb{Z}_2}$-ideal graduado gerado por $y_1y_2 - y_2y_1$ e $z_1z_2z_3 - z_3z_2z_1$ e por $F(M_2(\mathbb{K}))$ a subálgebra de $M_2(\mathbb{K}[y_i^{(j)}, z_i^{(j)}; i \geq 1, j = 1, 2])$, gerada pelas matrizes

$$A_i = \begin{pmatrix} y_i^{(1)} & y_i^{(2)} \\ by_i^{(2)} & y_i^{(1)} \end{pmatrix} \text{ e } B_i = \begin{pmatrix} z_i^{(1)} & z_i^{(2)} \\ -bz_i^{(2)} & -z_i^{(1)} \end{pmatrix}, \quad b \in \mathbb{K} - \mathbb{K}^2.$$

Notemos que j indica a diagonal da matriz na qual estão os elementos.

Proposição 6.3.20 *A álgebra graduada ${}^{\mathbb{K}\langle X\rangle}/_{T_{\mathbb{Z}_2}(M_2(\mathbb{K}))}$ é isormorfa à álgebra $F(M_2(\mathbb{K}))$. Quando $G = \mathbb{Z}_n$, o T_G-ideal é denotado por T_n.*

Demonstração: Defina as matrizes $Y_i = y_i^{(1)}(e_{11}+e_{22})+y_i^{(2)}(e_{12}+be_{21})$ e $Z_i = z_i^{(1)}(e_{11}-e_{22})+z_i^{(2)}(e_{12}-be_{21})$, em que $b \in \mathbb{K}-\mathbb{K}^2$. Repare que Y_i e Z_i são, respectivamente, A_i e B_i.

Então, defina $\varphi : \mathbb{K}\langle X\rangle \to F(M_2(\mathbb{K}))$, $\varphi(y_1, \cdots, y_n, z_1, \cdots z_n) \mapsto \varphi(Y_1, \cdots, Y_n, Z_1, \cdots Z_n)$, por $\varphi(y_i) = Y_i$ e $\varphi(z_i) = Z_i$. É fácil ver que, φ é um homomorfismo sobrejetor de álgebras e $Nuc(\varphi) = T_2(M_2(\mathbb{K}))$. Logo, pelo Teorema 5.2.6, a álgebra graduada $\mathbb{K}\langle X\rangle/T_2(M_2(\mathbb{K}))$ é isomorfa à álgebra $F(M_2(\mathbb{K}))$. ■

Essa proposição é utilizada na demonstração de um teorema da teoria de álgebras no qual é dada uma base para as identidades polinomiais graduadas. Além disso, podemos perceber que a álgebra graduada $\mathbb{K}\langle X\rangle/T_2(M_2(\mathbb{K}))$, na qual $\mathbb{K}\langle X\rangle$ é uma álgebra associativa livre G-graduada e $T_2(M_2(\mathbb{K}))$ um T-ideal de $\mathbb{K}\langle X\rangle$, trata-se de uma álgebra quociente, em especial, uma álgebra relativamente livre graduada.

Conclusão

Ao longo do trabalho vimos como é a construção do quociente em algumas estuturas algébricas. Começando pelos clássicos, estudamos essa construção nos grupos, anéis e espaços vetoriais, nossos conhecidos das disciplinas da graduação.

No Capítulo 5, no entanto, estudamos o quociente de uma estrutura um tanto estranha, a álgebra, que a grosso modo, podemos dizer que é um anel e um espaço vetorial ao mesmo tempo, uma vez que respeita as propriedades que definem essas duas estruturas simultaneamente.

Para a construção da álgebra quociente, tomamos uma álgebra R e uma subálgebra I ideal em R. Assim como fizemos nas demais estruturas, definimos uma relação de equivalência entre seus elementos, definimos as classes laterais, e por fim o conjunto das classes laterais de I com relação à R, denotado por

$$R/I = \{a + I;\ a \in I\}.$$

Nesse conjunto, definimos as operações de adição, multiplicação e multiplicação por escalar, mostrando que as mesmas estão bem definidas e, a partir daí, foi fácil verificar que o conjunto quociente das classes laterais é também uma álgebra, a álgebra quociente.

No capítulo seguinte buscamos nos aprofundar um pouco mais na teoria de álgebras e estudamos as álgebras com identidades polinomiais e as álgebras com identidades polinomiais graduadas. Ao final desse capítulo, trazemos um exemplo que une algumas definições vistas durante esses dois capítulo finais que desempenha um papel importante na teoria de álgebras.

Das observações feitas ao longo desse estudo, o que se pode dizer é que a construção do quociente em todas as estruturas segue um padrão. Em todas as construções foi necessário definir uma relação de equivalência entre os elementos do conjunto e definir as classes laterais à esquerda e a direita. Com exceção de grupos, nas demais estruturas as classes laterais à esquerda e à direita coincidiam.

Em todas as construções precisamos de subconjuntos, e em alguns deles possuiam característica especiais, como os subgrupos normais e os ideais, em grupos e anéis. A partir daí, definimos um conjunto que continha todas as classes laterais, chamado de conjunto quociente.

Dentro desse conjunto definimos operações que por sua vez obedeciam as mesmas propriedades que definiam os conjuntos trabalhados, o que fazia do conjunto quociente uma estrutura álgebrica como aquela que estava sendo estudada.

Percebe-se ainda que em alguns casos o quociente desempenha papéis importantes, como em anéis, quando transforma algo de dimensão infinita em algo de dimensão finita, ou em álgebras em que há um quociente que desempenha um papel importante na busca por geradores dos T-ideais da álgebra $M_2(\mathbb{K})$.

A ideia que fica a partir desse estudo, em especial a partir das semelhanças e diferenças observadas, é que podemos fazer essa ligações entre as estruturas algébricas ao estudá-las separadamente. Isso pode facilitar a compreensão. Essa ideia de fazer ligações entre as estruturas algébricas pode estender-se para outros conceitos, seja analisando as particularidades de cada uma ou analisando o que há em comum.

Referências Bibliográficas

[1] DRENSKY, V. *Free Algebras and PI - Algebras.* Springer - Verlag, Singapore **30**, 2000.

[2] DOMINGUES, H. H., IEZZI, G. *Álgebra Moderna.* 2ª edição. São Paulo: Saraiva, 1982.

[3] GARCIA, A., LEQUAIN, Y. *Elementos de Álgebra.* 2ª edição. Rio de Janeiro: Projeto Euclides, 2003.

[4] HALMOS, P. R. *Finite – Dimensional Vector Spaces.* New York: Springer, 1987.

[5] HOFFMAN, K., KUNZE, R. *Álgebra Linear.*1ª edição, São Paulo: Polígono, 1970.

[6] REIS, J. C. *Graduações e Identidades Graduadas para Álgebras de Matrizes.* Tese de Doutorado, Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica, São Paulo (2012).

[7] YARTEY, J. N. A. *Álgebra II.* Salvador: UFBA, Instituto de Matemática e Estatística; Superintendência de Educação a Distância, 2017.

Índice Remissivo