UNIVERSIDADE FEDERAL DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA

Monografia de Especialização

Semissimplicidade de anéis de grupos e o teorema de Perlis-Walker

Reyssila Franciane Dutra do Nascimento

Belo Horizonte
2017

UNIVERSIDADE FEDERAL DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA

Reyssila Franciane Dutra do Nascimento

Semissimplicidade de anéis de grupos e o teorema de Perlis-Walker

Monografia apresentada ao corpo docente de Pós-Graduação em Matemática do Instituto de Ciências Exatas da Universidade Federal de Minas Gerais, como parte dos requisitos para a obtenção do título de Especialista em Matemática.

Orientador: Rafael Bezerra dos Santos

Belo Horizonte
Julho de 2017

Aos meus pais,

Eliane e Francisco.

Agradecimentos

Agradeço a Deus pela força, perseverança e a luz nos momentos difíceis nesta caminhada. Agradeço especialmente ao meu professor orientador Rafael Bezerra dos Santos, pela disponibilidade, paciência, dedicação, atenção, e incentivo durante a elaboração do mesmo. Agradeço à professora Ana Cristina Vieira e ao professor Osnel Boche Cristo por participar da avaliação deste trabalho e das valiosas sugestões. Agradeço aos meus pais pelo apoio incondicional e aos familiares e amigos pelo companheirismo em todos os momentos.

Lista de Símbolos

$\mathbb{Z}$	anel dos números inteiros
$\mathbb{Q}$	corpo dos números racionais
$\mathbb{C}$	corpo dos números complexos
$G \simeq H$	G é isomorfo a H
$\mathcal{Z}(G)$	centro do grupo G
$Im(f)$	imagem de f
$Ker(f)$	núcleo de f
$dim_K A$	dimensão de A sobre K, como espaço vetorial
$char(R)$	característica do anel R
$\otimes$	produto tensorial
$\oplus$	soma direta
$\|G\|$	ordem do grupo G
$\langle a \rangle$	grupo gerado por a
C_n	grupo cíclico de ordem n
ϵ	aplicação de aumento
$\triangle(G)$	ideal de aumento, núcleo da aplicação de aumento
$Ann_r(X)$	anulador à direita de X
$R[x]$	anel de polinômios com coeficientes em R
$\overline{K}$	fecho algébrico de K
$[F : K]$	grau da extensão F sobre K
$deg(f(x))$	grau do polinômio $f(x)$
$\varphi(n)$	$\|\{d \in \mathbb{Z} : 1 \leq d \leq n, mdc(n,d) = 1\}\|$
$\Phi_d(x)$	polinômio ciclotômico de ordem d

Sumário

Resumo

Dados um anel R e um grupo G, considere o anel de grupo RG. Neste trabalho, baseado na referência [5], apresentaremos uma demonstração para o Teorema de Maschke obtida por Heinrich Maschke. Esse teorema dá condições necessárias e suficientes para que o anel de grupo RG seja semissimples. Como consequência, apresentamos o resultado principal do nosso estudo, o Teorema de Perlis-Walker, que caracteriza as componentes simples de KG, a álgebra de grupo de um grupo abeliano finito G sobre um corpo K, quando $char(K) \nmid |G|$.

Palavras-chaves: módulo, anel de grupo, semissimplicidade.

Abstract

Given a ring R and a group G, consider the group ring RG. In this work, based on [5], we presente a proof of Maschke's theorem obtained by Heinrich Maschke. This theorem gives necessary and sufficient conditions for the group ring RG to be semisimple. As a consequence, we present the main result of our study, the Perlis-Walker Theorem, which characterizes the simple components of KG, the group algebra of a finite abelian group G over a field K, when $char(K) \nmid |G|$.

Key Words: module, group ring, semisimplicity.

Introdução

Dado um anel associativo com unidade R e um grupo G é possível construir um R-módulo livremente gerado por G com a multiplicação definida distributivamente estendendo-se R-linearmente a multiplicação em G. Chamamos esse R-módulo de anel de grupo de G sobre R e o denotamos por RG. Se R é um anel comutativo, então RG possui uma estrutura de R-álgebra e chamamos RG de álgebra do grupo G sobre R. Além disso, RG é comutativo se, e somente se, R é comutativo e G é abeliano.

A estrutura de anel de grupo tem conexão direta tanto com a teoria dos grupos quanto com a teoria de anéis, uma vez que todos os resultados em anéis de grupo estão intimamente conectados com fatos provenientes de ambas teorias.

Um R-módulo é semissimples se todo R-submódulo é um somando direto e, como todo anel R é um módulo sobre si próprio, dizemos que R é um anel semissimples se é semissimples como R-módulo. Se M é um R-módulo semissimples, então M é uma soma direta de R-submódulos simples. Já um anel semissimples pode ser escrito como uma soma direta de um número finito de ideais minimais à esquerda. Além disso, esses ideais minimais à esquerda são gerados por elementos idempotentes.

Assim como temos condições para que R seja semissimples, também temos condições para que o anel de grupo RG seja semissimples. Vamos estabelecer

nesse trabalho condições necessárias e suficientes sobre o anel R e o grupo G para que o anel de grupo RG seja semissimples e, consequentemente, para que uma álgebra de grupo sobre um corpo K seja semissimples. Se G é um grupo abeliano de ordem n e K é um corpo tal que $char(K) \nmid n$, então KG será isomorfo à soma direta finita de extensões simples de K. Demonstrar esse resultado, conhecido como Teorema de Perlis-Walker, é o objetivo principal desta monografia.

Este trabalho está estruturado da seguinte forma:

No Capítulo 1, daremos uma visão geral de fatos básicos sobre módulos, álgebras de grupos e produto tensorial.

No Capítulo 2, iniciamos a teoria de anéis semissimples. Damos uma visão geral sobre elementos idempotentes em um anel e sua relação com anéis semissimples. Logo em seguida, por meio do Teorema de Maschke, concluímos que o anel de grupo RG é um anel semisimples se, e somente se, R é semissimples, $|G|$ é finita e invertível em R.

No Capítulo 3, utilizamos todas as informações dos capítulos anteriores para atacarmos diretamente o Teorema de Perlis-Walker e obter uma decomposição explícita das álgebras de grupos abelianos como soma direta de subálgebras simples. Encerraremos esta seção dando uma demonstração desse teorema e deixando a seguinte pergunta: se $RG \simeq RH$, então $G \simeq H$?

A principal referência para este trabalho é [5]. Indicamos ao leitor as referências [1], [3] e [4] para mais informações sobre teoria de anéis e grupos. A referência [2] é indicada para informações mais avançadas de Álgebra Linear.

Capítulo 1

Resultados Preliminares

1.1 Módulos e Álgebras

Salvo menção ao contrário, ao longo do trabalho, R denotará um anel associativo com identidade 1.

Definição 1.1.1. *Seja R um anel. Um grupo abeliano $(M, +)$ é chamado de um R-módulo (à esquerda) se para cada $r \in R$ e cada $m \in M$ corresponde um elemento $rm \in M$ tal que:*

(i) $(r + s)m = rm + sm$;

(ii) $r(m + n) = rm + rn$;

(iii) $(rs)m = r(sm)$;

(iv) $1m = m$,

para todos $r, s \in R$, $m, n \in M$.

De maneira análoga, podemos definir um R-módulo à direita. Utilizaremos a expressão R-módulo para nos referirmos a um R-módulo à esquerda.

Exemplo 1.1.2. *Quando $R = K$ é um corpo, os K-módulos são os K-espaços vetoriais.*

Exemplo 1.1.3. *Sejam $(G, +)$ um grupo abeliano e $n \in \mathbb{Z}$. Dado $g \in G$, defina:*

$$ng = \begin{cases} g + g + \ldots + g \quad (n \text{ vezes}), & \text{se} \quad n > 0; \\ (-g) + (-g) + \ldots + (-g) \quad (|n| \text{ vezes}), & \text{se} \quad n < 0; \\ 0, & \text{se} \quad n = 0. \end{cases}$$

Com a multiplicação assim definida, G é um $\mathbb{Z}$-módulo.

Exemplo 1.1.4. *Dado um anel A, seja $A^n := \underbrace{A \times A \times \cdots \times A}_{n-vezes}$. A^n possui uma estrutura de grupo abeliano definindo $a + b := (a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$, para todos $(a_1, a_2, \ldots, a_n)$, $(b_1, b_2, \ldots, b_n) \in A^n$. Agora, dados $x \in A$ e $b = (b_1, b_2, \ldots, b_n) \in A^n$, defina $xb = (xb_1, xb_2, \ldots, xb_n)$. Com a multiplicação assim definida, A^n é um A-módulo.*

De fato, dados $x, y \in A$ e $a = (a_1, a_2, \ldots, a_n)$, $b = (b_1, b_2, \ldots, b_n) \in A^n$, temos:

(i) $(x + y)a = ((x + y)a_1, (x + y)a_2, \ldots, (x + y)a_n) = (xa_1 + ya_1, xa_2 + ya_2, \ldots, xa_n + ya_n) = (xa_1, xa_2, \ldots, xa_n) + (ya_1, ya_2, \ldots, ya_n) = xa + ya.$

(ii) A verificação é semelhante ao item (i).

(iii) $(xy)a = ((xy)a_1, (xy)a_2, \ldots, (xy)a_n) = (x(ya_1), x(ya_2), \ldots, x(ya_n)) = x(ya_1, ya_2, \ldots, ya_n) = x(ya).$

(iv) Segue da definição de anel, pois $1a_i = a_i$ para todo $i \in \{1, \ldots, n\}$.

O exemplo a seguir pode ser generalizado para matrizes de ordem n.

Exemplo 1.1.5. *Dado R um anel comutativo, seja $(M_{2\times1}(R),+)$ o grupo das matrizes 2×1. Então $M_{2\times1}(R)$ é um $M_{2\times2}(R)$-módulo com a operação dada a seguir: dados $A=\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in M_{2\times2}(R)$ e $X=\begin{pmatrix} x_{11} \\ x_{21} \end{pmatrix} \in M_{2\times1}(R)$,*

$$AX := \begin{pmatrix} a_{11}x_{11}+a_{12}x_{21} \\ a_{21}x_{11}+a_{22}x_{21} \end{pmatrix},$$

a multiplicação usual de matrizes. Das propriedades da multiplicação de matrizes, $M_{2\times1}(R)$ é um $M_{2\times2}(R)$-módulo.

Exemplo 1.1.6. *Sejam R um anel e I um ideal à esquerda (à direita) de R. Então I é um R-módulo à esquerda (à direita). Em particular R pode ser visto como um módulo sobre si próprio. Para explicitar quando estaremos observando R como R-módulo à esquerda (à direita) utilizaremos a notação ${}_RR$ (R_R).*

Definição 1.1.7. *Seja M um R-módulo. Um subconjunto N não vazio de M é dito um R-submódulo (ou simplesmente um submódulo) de M se:*

(i) $(N,+)$ é um subgrupo de $(M,+)$;

(ii) Para todo $r\in R$ e todo $n\in N$, tem-se que $rn\in N$.

Lema 1.1.8. *Sejam M um R-módulo e N um subconjunto não-vazio de M. Então N é um R-submódulo de M se, e somente se, para todos $r\in R$, m, $n\in N$, $rm+n\in N$.*

Demonstração. Se N é um R-submódulo de M, então $rm+n\in N$, para todo $r\in R$, m, $n\in N$, pois N é um subgrupo de M. Reciprocamente, suponha que $rm+n\in N$. Temos, que $0\in N$, pois $0=(-1)n+n$. Logo, $rm\in N, \forall r\in R$, $m\in N$. Como $m-n\in N$, $\forall m$, $n\in N$, temos que N é um subgrupo de M e, portanto, um R-submódulo de M. □

Exemplo 1.1.9. *Seja V um espaço vetorial sobre um corpo K. Os K-submódulos de V são seus subespaços vetoriais.*

Exemplo 1.1.10. *Seja R um anel. Os submódulos de ${}_RR$ (R_R) são os seus ideais à esquerda (à direita). Esse fato será utilizado mais a frente, quando falarmos de semissimplicidade em anéis.*

Exemplo 1.1.11. *Sejam $M_2(R)$ o anel das matrizes 2×2 sobre um anel comutativo R e*

$$\mathcal{Z}(M_2(R)) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in R \right\}$$

o centro de $M_2(R)$. Temos que $\mathcal{Z}(M_2(R))$ é um R-submódulo de $M_2(R)$, mas $\mathcal{Z}(M_2(R))$ não é um $M_2(R)$-submódulo de $M_2(R)$, pois dados $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ e $\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$ em $M_2(R)$ e $\mathcal{Z}(M_2(R))$, respectivamente, o resultado da multiplicação dessas matrizes é $\begin{pmatrix} ax & bx \\ cx & dx \end{pmatrix} \notin \mathcal{Z}(M_2(R))$.

Definição 1.1.12. *Sejam M e N R-módulos. Uma aplicação $f : M \to N$ é um R-homomorfismo de módulos se, para todos m, $n \in M$ e $r \in R$, tem-se:*

(i) $f(m+n) = f(m) + f(n)$;

(ii) $f(rm) = rf(m)$.

Exemplo 1.1.13. *A aplicação $f : M \longrightarrow N$ tal que $f(m) = 0$, para todo $m \in M$, é um R-homomorfismo, para quaisquer R-módulos M e N.*

Exemplo 1.1.14. *Seja R um anel comutativo e M um R-módulo. Defina*

$$\begin{aligned} f_a : M &\longrightarrow M \\ m &\longmapsto am. \end{aligned}$$

Dados $m, n \in M$ temos:

$f_a(m+n) = a(m+n) = am + an = f_a(m) + f_a(n)$

$f_a(rm) = a(rm) = (ar)m = r(am) = rf_a(m)$

Portanto f_a é um R-homomorfismo.

Definição 1.1.15. *Dados M, N R-módulos, um R-homomorfismo $f : M \longrightarrow N$ é um R-isomorfismo se f é bijetor. Quando existir um R-isomorfismo entre M e N, diremos que M e N são isomorfos e escrevemos $M \simeq N$.*

Exemplo 1.1.16. *Se R é um anel comutativo e $a \in R$ é um elemento invertível, então*

$$\begin{aligned} f_a : M &\longrightarrow M \\ m &\longmapsto am. \end{aligned}$$

f_a é um R-isomorfismo.

Como vimos no Exemplo 1.1.14, f_a é um R-homomorfismo. Sejam m, $n \in M$. Se $f_a(m) = f_a(n)$ temos que $am = an$ e, como a é invertível, multiplicando a igualdade anterior por a^{-1} à esquerda, concluímos que $m = n$. Portanto f_a é injetora. Além disso, para todo $m \in M$, temos que $a^{-1}m \in M$ e $f_a(a^{-1}m) = m$. Portanto f é sobrejetora e, consequentemente, f_a é um R-isomorfismo.

Definição 1.1.17. *Dado $f : M \longrightarrow N$ um R-homomorfismo, chamam-se imagem de f e núcleo de f, respectivamente, os conjuntos:*

$Im(f) = \{f(m) : m \in M\}$;

$Ker(f) = \{m \in M : f(m) = 0\}$.

Exemplo 1.1.18. *Dados os $\mathbb{Z}$-módulos $\mathbb{Z}$ e $M_2(\mathbb{Z})$, considere a função $f : \mathbb{Z} \longrightarrow M_2(\mathbb{Z})$, dada por $f(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$. Claramente f é um $\mathbb{Z}$-homomorfismo e*

$$Ker(f) = \left\{ a \in \mathbb{Z} : f(a) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\} = \{0\}$$

$$Im(f) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{Z} \right\} = \mathcal{Z}(M_2(\mathbb{Z})).$$

Proposição 1.1.19. *Dado um R-homomorfismo $f : M \longrightarrow N$, temos que $Im(f)$ é um R-submódulo de N e o $Ker(f)$ é um R-submódulo de M.*

Demonstração. Primeiramente provemos que $Im(f)$ é um R-submódulo de N. Note que $Im(f) \neq \emptyset$, pois $0 \in Im(f)$. Se $Im(f) = \{0\}$ então segue o resultado. Se $Im(f) \neq \{0\}$, então existem x, $y \in Im(f)$. Logo, existem z, $w \in M$ tais que $f(z) = x$ e $f(w) = y$. Daí $rx + y = rf(z) + f(w) = f(rz) + f(w) = f(rz + w)$ para todo $r \in R$. Como M é um R-módulo, $rz + w \in M$, portanto $rx + y \in Im(f)$.

Agora mostremos que $Ker(f)$ é um R-submódulo de M. Temos que $0 \in Ker(f)$, logo $Ker(f) \neq \emptyset$. Se $Ker(f) = \{0\}$ temos o resultado. Se $Ker(f) \neq \{0\}$, então existem x, $y \in Ker(f)$. Dado $r \in R$, temos que $f(rx + y) = f(rx) + f(y) = rf(x) + f(y) = 0$. Como M é um R-módulo, $rx + y \in M$ e, portanto, $rx + y \in Ker(f)$. □

Proposição 1.1.20. *Sejam M, N R-módulos e $f : M \longrightarrow N$ um R-homomorfismo. Então f é injetora se, e somente se, $Ker(f) = \{0\}$.*

Demonstração. Suponha que f é injetora. Então, para qualquer $x \in M$, se $f(x) = 0$ temos que $x = 0$, pois $f(0) = 0$. Portanto $Ker(f) = \{0\}$.

Reciprocamente, suponha que $Ker(f) = \{0\}$. Dado x, $y \in M$, se $f(x) = f(y)$ temos $f(x) - f(y) = f(x - y) = 0$, assim $x - y \in Ker(f)$. Como $Ker(f) = \{0\}$ temos que $x - y = 0$, logo $x = y$. Portanto f é injetora.

□

Definição 1.1.21. *Seja N um submódulo do R-módulo M. O quociente M/N torna-se um R-módulo com a operação $r\overline{m} = \overline{rm}$, $r \in R$, $\overline{m} \in M/N$. Chamamos esse R-módulo de módulo fator M por N.*

A seguir, enunciamos o Teorema do Isomorfismo cuja demonstração é análoga para grupos e anéis.

Teorema 1.1.22. *Sejam M e N R-módulos e $f : M \longrightarrow N$ um R-homomorfismo. Então $\dfrac{M}{Ker(f)} \cong Im(f)$.*

Da teoria de espaços vetoriais, temos bem definidas a noção de base e dimensão. Como todo espaço vetorial é um módulo, é natural nos perguntarmos se estes conceitos podem ser estendidos para a classe dos R-módulos.

Definição 1.1.23. *Sejam R um anel e I um conjunto de índices. Dizemos que uma sequência $(r_i)_{i\in I}$ de elementos de R é quase-nula se apenas uma quantidade finita de elementos da sequência é não-nula.*

Definição 1.1.24. *Seja M um R-módulo. Um conjunto $\{x_i\}_{i\in I}$ de elementos de M é dito um conjunto gerador de M (ou dizemos que $\{x_i\}_{i\in I}$ gera M) se, para todo $m \in M$, exite uma sequência quase-nula $(r_i)_{i\in I}$ de elementos de R tal que $m = \sum_{i\in I} r_i x_i$. Se o conjunto $\{x_i\}_{i\in I}$ é finito, dizemos que M é finitamente gerado.*

Definição 1.1.25. *Seja M um R-módulo. Um conjunto $\{x_i\}_{i\in I}$ de elementos de M diz-se linearmente independente (ou livre) se para toda sequência quase-nula $(r_i)_{i\in I}$ de elementos de R tem-se que $\sum_{i\in I} r_i x_i = 0$ implica que $r_i = 0$ para todo $i \in I$.*

Definição 1.1.26. *Seja M um R-módulo. Um conjunto $\{x_i\}_{i\in I}$ de elementos de M diz-se uma R-base de M se $\{x_i\}_{i\in I}$ é um conjunto linearmente independente e gera M.*

Definição 1.1.27. *Um R-módulo M é chamado de livre se possui uma R-base.*

Exemplo 1.1.28. *Seja A um anel. O conjunto*

$$B = \{(1, 0, \ldots, 0), (0, 1, \ldots, 0), \ldots, (0, \ldots, 0, 1)\}$$

é uma A-base do A-módulo A^n. De fato, como $(a_1, \ldots, a_n) = a_1(1, 0, \ldots, 0) + \cdots + a_n(0, \ldots, 0, 1)$, temos que B gera A^n e facilmente podemos notar que B é linearmente independente. Portanto A^n é um A-módulo livre.

Exemplo 1.1.29. *O anel dos inteiros Gaussianos $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}, i^2 = -1\}$ é um $\mathbb{Z}$-módulo com a estrutura*

$$xm = xa + (xb)i \text{ e } m_1 + m_2 = (a + c) + (b + d)i$$

onde $x \in \mathbb{Z}$ e $m_1 = a + bi$, $m_2 = c + di \in \mathbb{Z}[i]$. O conjunto $B = \{1, i\}$ é uma $\mathbb{Z}$-base de $\mathbb{Z}[i]$, pois B gera $\mathbb{Z}[i]$ e é linearmente independente sobre $\mathbb{Z}$. Portanto, $\mathbb{Z}[i]$ é um $\mathbb{Z}$-módulo livre.

Exemplo 1.1.30. *Considere o $R \times R$-módulo $R \times R$ com a estrutura*

$$(m, n)(a, b) = (ma, nb); (m, n), (a, b) \in R \times R.$$

Então $R \times R$ é um $R \times R$-módulo livre gerado pelo conjunto $\{(1, 1)\}$.

Exemplo 1.1.31. *$\mathbb{Z}_n$ não é um $\mathbb{Z}$-módulo livre, pois todo conjunto em $\mathbb{Z}_n$ é linearmente dependente. De fato, dado $\overline{a} \in \mathbb{Z}_n$, existe $m \in \mathbb{Z} - \{0\}$ tal que $m\overline{a} = \overline{0}$.*

Diferentemente de espaços vetoriais, nem sempre duas R-bases de um R-módulo livre possuem o mesmo número de elementos. O exemplo a seguir ilustra essa afirmação.

Exemplo 1.1.32. *Considere o $\mathbb{Z}$-módulo $\mathbb{Z}[X]$ e o anel de endomorfismos $A := End_{\mathbb{Z}}\mathbb{Z}[X]$ com $(f+h)(p) = f(p)+h(p)$ e $(fh)(p) = f(h(p))$ para quaisquer f, $h \in A$ e $p \in \mathbb{Z}[X]$. O anel A é finitamente gerado como A-módulo, com conjunto gerador $\{1_A\}$ onde 1_A é a identidade do anel $End_{\mathbb{Z}}\mathbb{Z}[X]$. Observe que dado $f \in A$, se $f1_A = 0$ então $f = 0$. Assim esse conjunto unitário é uma A-base. Cada elemento $f \in A$ fica definido por sua imagem x^n, com $n \geq 0$, pois estes elementos formam uma $\mathbb{Z}$-base de $\mathbb{Z}[X]$. Defina f_1, $f_2 \in A$ da seguinte forma: para todo $n > 0$,*

$$\begin{cases} f_1(x^{2n+1}) = x^n \\ f_1(x^{2n}) = 0 \end{cases} \quad e \quad \begin{cases} f_2(x^{2n+1}) = 0 \\ f_2(x^{2n}) = x^n. \end{cases}$$

Vamos ver que $\{f_1, f_2\}$ é uma A-base de A.

Sejam α_1, $\alpha_2 \in A$ quaisquer. Se $\alpha_1 f_1 + \alpha_2 f_2 \equiv 0$, para todo $n > 0$, temos que $0 = (\alpha_1 f_1 + \alpha_2 f_2)(x^{2n+1}) = \alpha_1(f_1(x^{2n+1})) + \alpha_2(f_2(x^{2n+1})) = \alpha_1(x^n) + \alpha_2(0) = \alpha_1(x^n)$, pois α_2 é um homomorfismo.

Portanto $\alpha_1(p) = 0$ para todo $p \in \mathbb{Z}[X]$ e portanto $\alpha_1 \equiv 0$. Fazendo o mesmo cálculo para x^{2n}, obtemos $\alpha_2 \equiv 0$. Assim, a família $\{f_1, f_2\}$ é linearmente independente. Vejamos agora que a família é geradora. Seja $f \in A$ qualquer. Defina β_1, $\beta_2 \in A$ por $\beta_1(x^n) = f(x^{2n+1})$ e $\beta_2(x^n) = f(x^{2n})$, para todo $n > 0$, e estendemos estas aplicações linearmente a A. Verifiquemos que $f = \beta_1 f_1 + \beta_2 f_2$.

$(\beta_1 f_1 + \beta_2 f_2)(x^{2n+1}) = \beta_1(f_1(x^{2n+1})) + \beta_2(f_2(x^{2n+1})) = \beta_1(x^n) + \beta_2(0) = f(x^{2n+1})$.

Analogamente, $(\beta_1 f_1 + \beta_2 f_2)(x^{2n}) = f(x^{2n})$. Assim, e mais uma vez por linearidade, temos que $f = \beta_1 f_1 + \beta_2 f_2$.

Portanto, a família $\{f_1, f_2\}$ é também geradora e, assim, é uma A-base. Logo, $End_{\mathbb{Z}}\mathbb{Z}[X]$ admite bases como módulo sobre si próprio com cardinalidade distinta.

O teorema a seguir garante quando um R-módulo admite bases com a mesma cardinalidade.

Teorema 1.1.33. *Sejam R um anel comutativo e M um R-módulo livre finitamente gerado. Então quaisquer duas R-bases de M possuem o mesmo número de elementos.*

Definição 1.1.34. *Se M é um R-módulo livre e todas as R-bases de M possuem o mesmo número de elementos, a cardinalidade de uma R-base é chamada de posto de M e é denotada por posto(M).*

Exemplo 1.1.35. *Seja R um anel comutativo. Uma R-base para o R-módulo $R \times R$ é o conjunto $\{(1,0),(0,1)\}$. Como R é um anel comutativo e $R \times R$ é um R-módulo livre finitamente gerado, quaisquer duas R-bases de $R \times R$ possuem o mesmo número de elementos.*

Definição 1.1.36. *Seja R um anel comutativo. Um R-módulo A é chamado de uma R-álgebra (associativa) se existe uma multiplicação definida em A de tal maneira que com a adição em A e esta multiplicação, A é um anel e para todo $r \in R$, a,$b \in A$ é válida a seguinte condição: $r(ab) = (ra)b = a(rb)$.*

A condição que R seja comutativo é essencial. De fato, sejam R um anel não comutativo com identidade e $R[X]$ o anel de polinômios sobre R. Dados $p(x) = \sum_{i=1}^{t} a_i x^i$ e $q(x) = \sum_{j=1}^{s} b_j x^j \in R[X]$ com a_i, $b_j \in R$ para todo $1 \leq i \leq t$ e $1 \leq j \leq s$, temos que $p(x)q(x) = \sum_{i=1}^{t}\sum_{j=1}^{s} a_i b_j x^{i+j}$. Com esta multiplicação, $R[X]$ não é uma R-álgebra, pois, existem $0 \neq r \in R$, $p(x) = ax$, $q(x) = bx \in R[X]$, com $a, b \in R$ não nulos tal que $ar \neq ra \neq 0$ onde $r(p(x)q(x)) = r(abx^2) = (ra)bx^2 \neq (ar)bx^2 = a(rb)x^2 = p(x)(rq(x))$.

Definição 1.1.37. *Sejam R um anel comutativo e M uma R-álgebra. Um subconjunto não vazio $N \subseteq M$ é chamado de R-subálgebra de M se é um R-submódulo de M e para todo x, $y \in N$ temos que $xy \in N$.*

Exemplo 1.1.38. *Seja R um anel comutativo e considere o R-módulo $M_n(R)$. Com a multiplicação de matrizes, $M_n(R)$ é um anel. Além disso, note que $r(AB) = (rA)B = A(rB)$ para quaisquer $r \in R$ e $A, B \in M_n(R)$. Portanto, $M_n(R)$ é uma R-álgebra.*

Com relação ao exemplo acima, podemos observar que:

(i) Se R é um anel com unidade, então $M_n(R)$ é uma R-álgebra unitária.

(ii) $M_n(R)$ tem divisores de zero mesmo que R não possua divisores de zero. De fato, dada as matrizes $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ e $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ em $M_2(R)$ temos que $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

(iii) Uma matriz A em $M_n(R)$ é invertível se, e somente se, o determinante de A é uma unidade no anel R.

Exemplo 1.1.39. *O anel $\mathbb{Z}_n$ é uma $\mathbb{Z}$-álgebra com as operações de adição e multiplicação usuais. Dados $m \in \mathbb{Z}$ e $\overline{x}$, $\overline{y} \in \mathbb{Z}_n$ temos que: $m(\overline{x} \cdot \overline{y}) = m(\overline{xy}) = \overline{xy} + \overline{xy} + \cdots + \overline{xy} = \overline{xy + xy + \cdots + xy} = \overline{m(xy)} = \overline{(mx)y} = (m\overline{x})\overline{y}$. Por outro lado, $\overline{x}(m\overline{y}) = \overline{x}(\overline{y + \cdots + y}) = \overline{x(y + y + \cdots + y)} = \overline{xy + xy + \cdots + xy} = \overline{xy} + \overline{xy} + \cdots + \overline{xy} = m(\overline{xy}) = m(\overline{x} \cdot \overline{y})$. Logo, $(m\overline{x})\overline{y} = m(\overline{x} \cdot \overline{y}) = \overline{x}(m\overline{y})$ e $\mathbb{Z}_n$ é uma $\mathbb{Z}$-álgebra .*

Definição 1.1.40. *Sejam M, N R-álgebras. Dizemos que $f : M \longrightarrow N$ é um R-homomorfismo de R-álgebras se é um R-homomorfismo de R-módulos e $f(mn) = f(m)f(n)$ para todos $m, n \in M$. Se f é bijetora, dizemos que f é um R-isomorfismo de R-álgebras.*

Exemplo 1.1.41. *Seja R um anel comutativo. Com a operação de multiplicação de matrizes, $\mathcal{Z}(M_2(R))$ é uma R-subálgebra de $M_2(R)$. Defina a aplicação*

$$f : \mathcal{Z}(M_2(R)) \longrightarrow R \text{ dada por } f\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = a.$$

É fácil ver que f é um isomorfismo de R-álgebras, isto é, $\mathcal{Z}(M_2(R)) \simeq R$.

Definição 1.1.42. *Sejam K um corpo e A uma K-álgebra. Em particular A é um espaço vetorial sobre K. Definimos a dimensão de A sobre K, denotada por $dim_K A$, como sendo a dimensão de A sobre K como espaço vetorial.*

Exemplo 1.1.43. *Se K é um corpo, vimos que $\mathcal{Z}(M_2(K)) \simeq K$. Como $dim_K K = 1$, temos que $dim_K \mathcal{Z}(M_2(K)) = 1$.*

Definição 1.1.44. *Seja R um anel. A característica de R, denotada por $char(R)$, é o menor inteiro positivo n tal que $nr = 0$, para todo $r \in R$. Se tal elemento n não existe, dizemos que R tem característica 0.*

Exemplo 1.1.45. *$char(\mathbb{Z}_n) = n$.*

Suponha que exista um corpo F tal que $char(F) = 6$. Então $6r = 0$ para todo $r \in F$. Daí, $0 = 6r = (2 \cdot 3)r = 2(3r)$ logo, $3r = 0$ para todo $r \in F$. Absurdo, pois contraria a minimalidade da característica do corpo F.

Utilizando este argumento, temos o seguinte resultado.

Teorema 1.1.46. *A característica de um corpo K é 0 ou é um número primo.*

Corolário 1.1.47. *Se K um corpo finito, então a característica de K é prima.*

Demonstração. Segue do fato que em todo corpo finito todos os elementos possuem ordem aditiva finita. Logo, a característica de um corpo finito não pode ser 0. Portanto, pelo teorema anterior, a característica de um corpo finito é prima. □

O exemplo a seguir mostra que corpos de característica finita não necessariamente tem cardinalidade finita.

Exemplo 1.1.48. *Dado $p \in \mathbb{Z}$, p primo, considere $\mathbb{Z}_p$, o corpo dos inteiros módulo p. Considere o corpo de frações de $\mathbb{Z}_p[x]$,*

$$\mathbb{Z}_p(x) = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{Z}[x], g(x) \neq 0 \right\}.$$

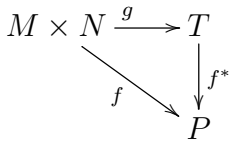
Temos que $\mathbb{Z}_p(x)$ é infinito, pois contém 1, x, x^2, ..., e sua característica é p, pois estamos olhando polinômios com coeficientes em $\mathbb{Z}_p$.

1.2 Produto Tensorial

Nesta seção, mostraremos a importante construção do produto tensorial. Nesta seção o anel R sobre o qual trabalharemos é comutativo com unidade.

Sejam R um anel e M, N, P R-módulos. Uma aplicação $f : M \times N \longrightarrow P$ é chamada de R-bilinear se: $f(r_1m_1 + r_2m_2, n) = r_1f(m_1, n) + r_2f(m_2, n)$, $f(m, r_1n_1 + r_2n_2) = r_1f(m, n_1) + r_2f(m, n_2)$ para todos m, m_1, $m_2 \in M$, n, n_1, $n_2 \in N$ e r_1, $r_2 \in R$.

Proposição 1.2.1. *Sejam M, N R-módulos. Então existe um único par (T, g), a menos de isomorfismos, consistindo de um R-módulo T e uma aplicação $g : M \times N \longrightarrow T$, R-bilinear, com a seguinte propriedade: dado qualquer R-módulo P e qualquer aplicação R-bilinear $f : M \times N \longrightarrow P$, existe uma única aplicação R-linear $f^* : T \longrightarrow P$, tal que $f = f^* \circ g$ (em outras palavras, toda função bilinear de $M \times N \longrightarrow P$ é fatorável).*



Demonstração. (Unicidade) Observe primeiramente que no diagrama abaixo temos que $g = g^* \circ g$, onde $g^* = id_T : T \longrightarrow T$ é a aplicação identidade. Logo, se existe $g^* : T \longrightarrow T$ tal que $g = g^* \circ g$, da unicidade de g^*, concluímos que $g^* = id_T$.

$$\begin{array}{ccc} M \times N & \xrightarrow{g} & T \\ & \searrow^{g} & \downarrow{\scriptstyle g^*} \\ & & T \end{array}$$

Suponha que exista um outro par (T', g') nas condições da proposição.

$$\begin{array}{ccc} M \times N & \xrightarrow{g'} & T' \\ & \searrow^{g} & \downarrow{\scriptstyle g^*} \\ & & T \end{array} \qquad \begin{array}{ccc} M \times N & \xrightarrow{g} & T \\ & \searrow^{g'} & \downarrow{\scriptstyle (g')^*} \\ & & T' \end{array}$$

Afirmação: g^* e $(g')^*$ são isomorfismos de R-módulos. De fato, por um lado, $g' = (g')^* \circ g = (g')^* \circ (g^* \circ g') = ((g')^* \circ g^*) \circ g'$. Portanto, pela unicidade, $(g')^* \circ g^* = id_{T'}$. Por outro lado, $g = g^* \circ g' = g^* \circ ((g')^* \circ g) = (g^* \circ (g')^*) \circ g$. Portanto $g^* \circ (g')^* = id_T$. Portanto $g^* = ((g')^*)^{-1}$ e assim, g^* é um isomorfismo de R-módulos.

(Existência) Seja B o R-módulo livremente gerado por $M \times N$, ou seja, os elementos de B são da forma $\sum_{i \in I} r_i(m_i, n_i), r_i \in R$.

Seja C o R-submódulo de B gerado pelos elementos

- $(m_1 + m_2, n) - (m_1, n) - (m_2, n)$
- $(m, n_1 + n_2) - (m, n_1) - (m, n_2)$
- $(rm, n) - r(m, n)$
- $(m, rn) - r(m, n)$

para todos m, m_1, $m_2 \in M$, n, n_1, $n_2 \in N$ e $r \in R$.

Seja $T = B/C$. Vamos denotar por $m \otimes n$ a classe de (m, n) em T. Logo, todo elemento de T é da forma $\sum_{i \in I} r_i(m_i \otimes n_i)$, $r_i \in R$.

Observe que

- $(m_1 + m_2) \otimes n = m_1 \otimes n - m_2 \otimes n$
- $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$
- $(rm) \otimes n = r(m \otimes n) = m \otimes (rm)$

para todos m, m_1, $m_2 \in M$, n, n_1, $n_2 \in N$ e $r \in R$.

Seja $f : M \times N \to P$ uma aplicação R-bilinear qualquer. Estendendo f R-linearmente a B, obtemos uma aplicação R-linear

$$\overline{f} : B \longrightarrow P$$
$$\sum_{i \in I} r_i(m_i, n_i) \longmapsto \sum_{i \in I} r_i f(m_i, n_i).$$

Seja $g : M \times N \longrightarrow T$ definida por $g(m, n) = m \otimes n$. Claramente g é R-bilinear. Defina $f^* : T \longrightarrow P$ por $f^*(m \otimes n) = \overline{f}(m, n)$ e estenda-a R-linearmente a T. A aplicação f^* está bem definida, pois como f é R-bilinear, temos que $\overline{f}$ se anula em todos os elementos de C e é R-linear. Agora, queremos mostrar que $f^* \circ g = f$. Dado $(m, n) \in M \times N$ temos que $(f^* \circ g)(m, n) = f^*(g(m, n)) = f^*(m \otimes n) = \overline{f}(m, n) = f(m, n)$. A aplicação f^* é única, pois a definimos nos geradores de B. Portanto o par (T, g) satisfaz as condições da proposição. □

O R-módulo T construído acima é chamado de produto tensorial de M e N e é denotado por $M \otimes_R N$, ou apenas $M \otimes N$ se não houver ambiguidade sobre o anel R. Ele é gerado, como R-módulo, pelos "produtos" $x \otimes y$. Se $\{x_i\}_{i \in I}$, $\{y_j\}_{j \in J}$ são famílias de geradores de M e N, respectivamente, sobre R, então os elementos $x_i \otimes y_j$ geram $M \otimes N$ sobre R. Em particular, se M e N são finitamente gerados, $M \otimes N$ também será.

Exemplo 1.2.2. *Dados quaisquer R-módulos M, N, temos que, em $M \otimes_R N$,*

(i) $m \otimes 0 = 0 \otimes n$, *pois* $m \otimes 0 = m \otimes (0n) = (0m) \otimes n = 0 \otimes n \ \forall m \in M$ *e* $n \in N$.

(ii) $m \otimes 0 = 0 \otimes 0$, *pois* $0 \otimes 0 = (0m) \otimes 0 = m \otimes (0 \cdot 0) = m \otimes 0 \ \forall m \in M$.

Exemplo 1.2.3. $\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n \simeq \mathbb{Z}_d$, *onde* $d = mdc(m, n)$. *Em particular, se* $1 = mdc(m, n)$, *então* $\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n = \{0\}$.

Seja $f : \mathbb{Z}_m \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_d$, tal que $f(x + \langle m\rangle, y + \langle n\rangle) = xy + \langle d\rangle$, onde $d = mdc(m, n)$.

Afirmação 1: f está bem definida.

De fato, dados $x_1 + \langle m\rangle$, $x_2 + \langle m\rangle \in \mathbb{Z}_m$ e $y_1 + \langle n\rangle$, $y_2 + \langle n\rangle \in \mathbb{Z}_n$, se $(x_1+\langle m\rangle, y_1+\langle n\rangle) = (x_2+\langle m\rangle, y_2+\langle n\rangle) \Rightarrow ((x_1-x_2)+\langle m\rangle, (y_1-y_2)+\langle m\rangle) = (\langle m\rangle, \langle n\rangle) \Rightarrow x_1-x_2 \in \langle m\rangle$ e $y_1-y_2 \in \langle n\rangle$. Assim, existem k_1, $k_2 \in \mathbb{Z}$ tais que $(x_1-x_2) = mk_1$ e $(y_1-y_2) = nk_2$. Como d é o $mdc(m, n)$, existem q_1 e $q_2 \in \mathbb{Z}$ tais que $m = dq_1$ e $n = dq_2$. Daí, $(x_1 - x_2) = (dq_1)k_1$ e $(y_1 - y_2) = (dq_2)k_2$, logo $(x_1 - x_2) = d(q_1k_1)$ e $(y_1 - y_2) = d(q_2k_2) \Rightarrow d|(x_1 - x_2)$ e $d|(y_1 - y_2)$. Como y_1 e $x_2 \in \mathbb{Z}$, temos $d|(x_1 - x_2)y_1$, $d|(y_1 - y_2)x_2$ e consequentemente $d|(x_1y_1 - x_2y_2)$. Logo $(x_1y_1 - x_2y_2) + \langle d\rangle = \langle d\rangle \Rightarrow x_1y_1 + \langle d\rangle = x_2y_2 + \langle d\rangle$.

Afirmação 2: f é $\mathbb{Z}$-bilinear.

De fato, dados $x_1 + \langle m\rangle$, $x_2 + \langle m\rangle \in \mathbb{Z}_m$ e $y_1 + \langle n\rangle$, $y_2 + \langle n\rangle \in \mathbb{Z}_n$ e $\alpha \in \mathbb{Z}$, temos: $f(\alpha(x_1 + \langle m\rangle) + (x_2 + \langle m\rangle), y + \langle n\rangle) = f((\alpha x_1 + x_2) + \langle m\rangle, y + \langle n\rangle) = (\alpha x_1 + x_2)y + \langle d\rangle = (\alpha x_1 y + x_2 y) + \langle d\rangle = (\alpha x_1 y + \langle d\rangle) + (x_2 y + \langle d\rangle) = \alpha(x_1 y + \langle d\rangle) + (x_2 y + \langle d\rangle) = \alpha f(x_1 + \langle m\rangle, y + \langle n\rangle) + f(x_2 + \langle m\rangle, y + \langle n\rangle)$. Analogamente verifica-se que $f(x + \langle m\rangle, \alpha(y_1 + \langle n\rangle) + (y_2 + \langle n\rangle)) = \alpha f(x + \langle m\rangle, y_1 + \langle n\rangle) + f(x + \langle m\rangle, y_2 + \langle n\rangle)$.

Portanto, pela Proposição 1.2.1 existe uma aplicação $\mathbb{Z}$-linear $f^* : \mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n \longrightarrow \mathbb{Z}_d$ que satisfaz $f = f^* \circ g$, onde $g : \mathbb{Z}_m \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n$ e

$g(x + \langle m\rangle, y + \langle n\rangle) = (x + \langle m\rangle) \otimes (y + \langle n\rangle)$.

Defina $w : \mathbb{Z}_d \longrightarrow \mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n$ tal que $w(z + \langle d\rangle) = (1 + \langle m\rangle) \otimes (z + \langle n\rangle)$.

Afirmação 3: w está bem definida.

Dados $z_1+\langle d\rangle$ e $z_2+\langle d\rangle \in \mathbb{Z}_d$, se $z_1+\langle d\rangle = z_2+\langle d\rangle \Rightarrow z_1-z_2 \in \langle d\rangle \Rightarrow \exists k \in \mathbb{Z}$ tal que $z_1 - z_2 = dk \Rightarrow z_1 = z_2 + dk$. Daí, $w(z_1 + \langle d\rangle) = (1 + \langle m\rangle) \otimes (z_1 + \langle n\rangle) = (1 + \langle m\rangle) \otimes ((z_2 + dk) + \langle n\rangle)$. Como $d = mdc(m, n)$, existem inteiros r, s tais que $d = rm + sn$. Logo, $w(z_1 + \langle d\rangle) = (1 + \langle m\rangle) \otimes (z_2 + dk + \langle n\rangle) = (1 + \langle m\rangle) \otimes (z_2 + rmk + snk + \langle n\rangle) = (1 + \langle m\rangle) \otimes ((z_2 + \langle n\rangle) + (rmk + \langle n\rangle)) = ((1 + \langle m\rangle) \otimes (z_2 + \langle n\rangle)) + ((1 + \langle m\rangle) \otimes (rmk + \langle n\rangle)) = ((1 + \langle m\rangle) \otimes (z_2 + \langle n\rangle)) + ((m + \langle m\rangle) \otimes (rk + \langle n\rangle)) = (1 + \langle m\rangle) \otimes (z_2 + \langle n\rangle) = w(z_2 + \langle d\rangle)$.

Afirmação 4: w é $\mathbb{Z}$-homomorfismo.

Dados $z_1+\langle d\rangle$, $z_2+\langle d\rangle \in \mathbb{Z}_d$ e $z \in \mathbb{Z}$ temos que $w(z(z_1+\langle d\rangle)+(z_2+\langle d\rangle)) = w((zz_1+z_2)+\langle d\rangle) = (1+\langle m\rangle)\otimes((zz_1+z_2)+\langle n\rangle) = ((1+\langle m\rangle)\otimes(zz_1+\langle n\rangle))+((1+\langle m\rangle)\otimes(z_2+\langle n\rangle)) = z((1+\langle m\rangle)\otimes(z_1+\langle n\rangle))+(1+\langle m\rangle)\otimes(z_2+\langle n\rangle) = zw_1(z_1 + \langle d\rangle) + w(z_2 + \langle d\rangle)$.

Observe que $w \circ f^*((x + \langle m\rangle) \otimes (y + \langle n\rangle)) = w(xy + \langle d\rangle) = (1 + \langle m\rangle) \otimes (xy+\langle n\rangle) = x((1+\langle m\rangle)\otimes(y+\langle n\rangle) = (x+\langle m\rangle)\otimes(y+\langle n\rangle)$ e $f^* \circ w(z+\langle d\rangle) = f^*((1 + \langle m\rangle) \otimes (z + \langle n\rangle)) = 1.z + \langle d\rangle = z + \langle d\rangle$.

Portanto, f^* é um isomorfismo e $\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n \simeq \mathbb{Z}_d$.

O lema a seguir será utilizado na demonstração do Teorema de Perlis-Walker.

Lema 1.2.4. *Seja M um R-módulo à esquerda. Então $R \otimes_R M \simeq M$.*

Demonstração. Como M e R são R-módulos, exite um único par $(R\otimes_R M, q)$ a menos de isomorfismos, consistindo de um R-módulo $R\otimes M$ e uma aplicação R-bilinear $q : R \times M \longrightarrow R \otimes_R M$ definida por $q(r, m) = r \otimes m$. Seja $f : R \times M \longrightarrow M$ a aplicação R-bilinear dada por $f(r, m) = rm$. Então, existe uma única aplicação R-linear $f^* : R \otimes_R M \longrightarrow M$ tal que $f = f^* \circ q$.

Afirmação: f^* é um R-isomorfismo. De fato, defina

$$(f^*)' : M \longrightarrow R \otimes_R M$$
$$m \longmapsto 1_R \otimes m.$$

A aplicação $(f^*)'$ é R-homomorfismo, pois, $(f^*)'(m_1 + m_2) = 1_R \otimes (m_1 + m_2) = 1_R \otimes m_1 + 1_R \otimes m_2 = (f^*)'(m_1) + (f^*)'(m_2)$ e $(f^*)'(rm) = 1_R \otimes (rm) = r(1 \otimes m) = r(f^*)'(m)$ para todo m, m_1, $m_2 \in M$ e $r \in R$.

Além disso, $(f^* \circ (f^*)')(m) = f^*(1_R \otimes m) = 1_R m = m$, $\forall m \in M$. Por outro lado, $((f^*)' \circ f^*)(r \otimes m) = (f^*)'(rm) = 1_R \otimes (rm) = r \otimes m$, para todo $m \in M$, $r \in R$. Segue disso que, $(f^*)' \circ f^* = Id_{R \otimes_R M}$ e $f^* \circ (f^*)' = Id_M$. Portanto, f^* é isomorfismo, que demonstra o lema.

□

Proposição 1.2.5. *Sejam M, M', N e N' R-módulos. Se $f : M \longrightarrow M'$ e $g : N \longrightarrow N'$ são homomorfismos de R-módulos, então existe um único homomorfismo $h := f \otimes g : M \otimes_R N \longrightarrow M' \otimes_R N'$ dado por $h(m \otimes n) = f(m) \otimes g(n)$.*

Demonstração. Defina $\alpha : M \times N \longrightarrow M' \otimes_R N'$ por $\alpha(m, n) = f(m) \otimes g(n)$. A aplicação α é R-bilinear, pois $\alpha(rm_1 + m_2, n) = f(rm_1 + m_2) \otimes g(n) = (f(rm_1) + f(m_2)) \otimes g(n) = f(rm_1) \otimes g(n) + f(m_2) \otimes g(n) = rf(m_1) \otimes g(n) + f(m_2) \otimes g(n) = r\alpha(m_1, n) + \alpha(m_2, n)$ e $\alpha(m, rn_1 + n_2) = f(m) \otimes g(rn_1 + n_2) = f(m) \otimes g(rn_1) + f(m) \otimes g(n_2) = r(f(m) \otimes g(n_1)) + f(m) \otimes g(n_2) = r\alpha(m, n_1) + \alpha(m, n_2)$ para todos m, m_1, $m_2 \in M$, n, n_1, $n_2 \in N$ e $r \in R$. Pela propriedade universal de produto tensorial, existe um único homomorfismo $\alpha^* : M \otimes_R N \longrightarrow M' \otimes_R N'$ onde $\alpha^*(m \otimes n) = f(m) \otimes g(n)$. □

Definição 1.2.6. *Sejam M um R-módulo e $\{M_i\}_{i \in I}$ uma família de submódulos de M. Então a soma dos submódulos $\sum_{i \in I} M_i$ é o conjunto das somas $\sum_{i \in I} x_i$ com $x_i \in M_i$ e $x_i = 0$, exceto para uma quantidade finita de índices.*

Definição 1.2.7. *Seja $\{M_i\}_{i\in I}$ uma família de submódulos de um R-módulo M. Dizemos que M é soma direta dos submódulos dessa família, e escrevemos $M = \oplus_{i\in I} M_i$, se:*

(i) $M = \sum_{i\in I} M_i$;

(ii) $M_i \cap \left(\sum_{j\neq i} M_j \right) = 0$, *para todo* $i \in I$.

Proposição 1.2.8. *Sejam M_1, M_2 e N R-módulos. Então*

$$(M_1 \oplus M_2) \otimes_R N \simeq (M_1 \otimes_R N) \oplus (M_2 \otimes_R N).$$

Demonstração. Consideremos $i_1 : M_1 \hookrightarrow M_1 \oplus M_2$ e $i_2 : M_2 \hookrightarrow M_1 \oplus M_2$ as imersões canônicas e $id_N : N \to N$ a aplicação identidade de N. Pela Proposição 1.2.5, existem únicos R-homomorfismos α_1 e α_2 tais que $\alpha_1 = i_1 \otimes id_N$ e $\alpha_2 = i_2 \otimes id_N$. Seja $\alpha : (M_1 \otimes N) \oplus (M_2 \otimes N) \longrightarrow (M_1 \oplus M_2) \otimes N$ definida por $\alpha(m_1 \otimes n_1, m_2 \otimes n_2) = \alpha_1(m_1 \otimes n_1) + \alpha_2(m_2 \otimes n_2)$. Como α_1 e α_2 são R-homomorfismos, temos que α é um R-homomorfismo.

Agora, consideremos $\pi_1 : M_1 \times M_2 \longrightarrow M_1$ e $\pi_2 : M_1 \times M_2 \longrightarrow M_2$ as projeções canônicas e, novamente, pela Proposição 1.2.5, existem únicos R-homomorfismos β_1 e β_2 tais que $\beta_1 = \pi_1 \otimes id_N$ e $\beta_2 = \pi_2 \otimes id_N$. Defina $\beta : (M_1 \oplus M_2) \otimes N \longrightarrow (M_1 \otimes N) \oplus (M_2 \otimes N)$ por $\beta((m_1, m_2) \otimes n) = \beta_1((m_1, m_2) \otimes n) + \beta_2((m_1, m_2) \otimes n)$. Temos que β é um R-homomorfismo e β é a inversa de α, pois

$(\alpha \circ \beta)((m_1, m_2) \otimes n) = \alpha((m_1 \otimes n) + (m_2 \otimes n)) = (m_1, m_2) \otimes n$ e

$(\beta \circ \alpha)((m_1 \otimes n) + (m_2 \otimes n)) = \beta((m_1, m_2) \otimes n) = (m_1 \otimes n) + (m_2 \otimes n)$.

Portanto, $(M_1 \oplus M_2) \otimes_R N \simeq (M_1 \otimes_R N) \oplus (M_2 \otimes_R N)$. □

Corolário 1.2.9. $(\oplus_{i\in I} M_i) \otimes_R N \simeq \oplus_{i\in I}(M_i \otimes_R N)$

Sejam M e N R-álgebras. Como M, N são R-módulos, podemos formar o produto tensorial $M \otimes_R N$, que é um R-módulo. Agora vamos definir uma multiplicação em $M \otimes_R N$.

Considere a aplicação $h : (M \times N) \times (M \times N) \longrightarrow M \otimes_R N$ definida por $(m_1, n_1, m_2, n_2) \longmapsto m_1 m_2 \otimes n_1 n_2$. Temos que h é 4-multilinear, ou seja, é R-linear em cada fator. É possível mostrar que existe uma aplicação R-bilinear $f : (M \otimes_R N) \times (M \otimes_R N) \longrightarrow M \otimes_R N$ tal que $f(m \otimes n, m' \otimes n') = mm' \otimes nn'$.

Naturalmente, poderíamos ter escrito esta fórmula diretamente, mas sem algum argumento como nós demos, não haveria garantia de que estaria bem definida, portanto, uma multiplicação no produto tensorial $D = M \otimes_R N$ dada por

$$\left(\sum_i (m_i \otimes n_i)\right)\left(\sum_j (m'_j \otimes n'_j)\right) = \sum_{i,j}((m_i m'_j) \otimes (n_i n'_j)).$$

Com isso, temos que $M \otimes_R N$ é uma R-álgebra.

1.3 Anéis de Grupos

Definição 1.3.1. *Sejam G um grupo e R um anel. O anel de grupo de G sobre R, denotado por RG, é o R-módulo livremente gerado por G com a multiplicação definida distributivamente estendendo-se R-linearmente a multiplicação em G.*

Assim, RG consiste de todas as combinações lineares formais finitas da forma $\alpha = \sum_{g \in G} a_g g$, com $a_g \in R$. Se $\beta = \sum_{g \in G} b_g g \in RG$ e $r \in R$, então a adição, multiplicação e a multiplicação por elementos de R em RG são definidas por:

$$\alpha + \beta = \sum_{g \in G} a_g g + \sum_{g \in G} b_g g \qquad = \sum_{g \in G} (a_g + b_g) g$$

$$\alpha\beta = \left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right) = \sum_{g,h\in G}(a_g b_h)(gh)$$
$$r\alpha = r\left(\sum_{g\in G} a_g g\right) \qquad = \sum_{g\in G}(ra_g)g.$$

Segue da definição que $\alpha = \beta$ se, e somente se, $a_g = b_g$, para todo $g \in G$.

Observe que RG é um anel com identidade $1_{RG} = 1_R 1_G$, que de agora em diante denotaremos por 1.

Se R é comutativo e G é finito temos que o posto de RG sobre R está bem definido e é igual a ordem de G. Também, utilizando o monomorfismo de anéis $\zeta : R \longrightarrow RG$ definido por $\zeta(r) = r1_G$, podemos considerar R como um subanel de RG.

Definição 1.3.2. *Dado* $\alpha = \sum_{g\in G} a_g g \in RG$, *o conjunto*

$$supp(\alpha) = \{g \in G; a_g \neq 0\}$$

é chamado de suporte de α. *Em outras palavras,* $supp(\alpha)$ *é o conjunto dos elementos de* G *que aparecem efetivamente na representação de* α.

Exemplo 1.3.3. *Sejam* $C_2 = \langle g : g^2 = 1\rangle$ *o grupo cíclico de ordem* 2 *e o corpo* $\mathbb{Z}_3$. *O anel de grupo de* C_2 *sobre* $\mathbb{Z}_3$ *é:*

$$\mathbb{Z}_3C_2 = \{a1_{C_2} + bg : a, b \in \mathbb{Z}_3\} = \{0, 1, 2, g, 2g, 1+g, 1+2g, 2+g, 2+2g\}.$$

Sejam $a = 1 + 2g$ *e* $b = 2 + g \in \mathbb{Z}_3C_2$. *Então,* $ab = (1+2g)(2+g) = 2 + g + 4g + 2g^2 = 2 + 2g + 2 = 1 + 2g$ *e* $a + b = (1 + 2g) + (2 + g) = 0$.

Exemplo 1.3.4. *O anel de grupo de* S_3 *sobre* $\mathbb{Z}_5$ *é*

$$\mathbb{Z}_5S_3 = \left\{\sum a_f f : a_f \in \mathbb{Z}_5, f \in S_3\right\}.$$

Sejam $\alpha = (12)$, $\beta = (12) + 2(123)$ *e* $\gamma = 3 \in \mathbb{Z}_5S_3$. *Então* $\alpha\beta = (12)((12) + 2(123)) = (12)(12) + 2(12)(123) = 1 + 2(23)$, $\beta\alpha = ((12) + 2(123))(12) = (12)(12) + 2(123)(12) = 1 + 2(13)$ *e* $\gamma\alpha + \beta = 3(12) + (12) + 2(123) = 4(12) + 2(123)$.

O próximo resultado será muito importante para demonstrar o Teorema de Perlis-Walker.

Proposição 1.3.5. *Sejam R um anel comutativo e G, H grupos. Então $R(G \times H) \simeq RG \otimes_R RH$.*

Demonstração. Considere

$$\begin{aligned} f : RG \times RH &\longrightarrow R(G \times H) \\ \left(\sum_{g \in G} a_g g, \sum_{h \in H} b_h h \right) &\longmapsto \sum_{\substack{g \in G \\ h \in H}} a_g b_h (g, h) \end{aligned}$$

f é uma aplicação R-bilinear. De fato,

$$\begin{aligned} f\left(\sum_{g \in G} a_g g + r \sum_{g \in G} c_g g, \sum_{h \in H} b_h h \right) &= f\left(\sum_{g \in G} (a_g + r c_g) g, \sum_{h \in H} b_h h \right) \\ &= \sum_{\substack{g \in G \\ h \in H}} (a_g + r c_g) b_h (g, h) \\ &= \sum_{\substack{g \in G \\ h \in H}} (a_g b_h + r c_g b_h)(g, h) \\ &= \sum_{\substack{g \in G \\ h \in H}} a_g b_h (g, h) + \sum_{\substack{g \in G \\ h \in H}} r(c_g b_h (g, h)) \\ &= \sum_{\substack{g \in G \\ h \in H}} a_g b_h (g, h) + r \sum_{\substack{g \in G \\ h \in H}} c_g b_h (g, h) \\ &= f\left(\sum_{g \in G} a_g g, \sum_{h \in H} b_h h \right) + r f\left(\sum_{g \in G} c_g g, \sum_{h \in H} b_h h \right). \end{aligned}$$

Analogamente verifica-se que

$$f\left(\sum_{g \in G} a_g g, \sum_{h \in H} b_h h + r \sum_{h \in H} d_h h \right) = f\left(\sum_{g \in G} a_g g, \sum_{h \in H} b_h h \right) + r f\left(\sum_{g \in G} a_g g, \sum_{h \in H} d_h h \right).$$

Como f é uma aplicação R-bilinear, pela propriedade do produto tensorial, existe um único homomorfismo de R-módulos

$$f^* : RG \otimes_R RH \longrightarrow R(G \times H)$$

tal que $f = f^* \circ g$, onde

$$g : RG \times RH \longrightarrow RG \otimes_R RH.$$
$$\left(\sum_{g\in G} r_g g, \sum_{h\in H} r_h h\right) \longmapsto \left(\sum_{g\in G} r_g g\right) \otimes \left(\sum_{h\in H} r_h h\right)$$

Defina

$$w : R(G \times H) \longrightarrow RG \otimes_R RG$$
$$\sum_{\substack{g\in G\\ h\in H}} r_{gh}(g,h) \longmapsto \sum_{\substack{g\in G\\ h\in H}} r_{gh}(g \otimes h).$$

w é um R-homomorfismo. De fato, dados $g \in G$, $h \in H$ e a_{gh}, $b_{gh} \in R$,

$$w\left(\left(\sum_{\substack{g\in G\\ h\in H}} a_{gh}(g,h)\right) + r\left(\sum_{\substack{g\in G\\ k\in H}} b_{gh}(g,h)\right)\right) = w\left(\sum_{\substack{g\in G\\ h\in H}} (a_{gh} + rb_{gh})(g,h)\right) =$$

$$\sum_{\substack{g\in G\\ h\in H}} (a_{gh} + rb_{gh})(g \otimes h) = \sum_{\substack{g\in G\\ h\in H}} a_{gh}(g \otimes h) + \sum_{\substack{g\in G\\ h\in H}} rb_{gh}(g \otimes h) =$$

$$\sum_{\substack{g\in G\\ h\in H}} a_{gh}(g \otimes h) + r \sum_{\substack{g\in G\\ h\in H}} b_{gh}(g \otimes h) = w\left(\sum_{\substack{g\in G\\ h\in H}} a_{gh}(g,h)\right) + rw\left(\sum_{\substack{g\in G\\ h\in H}} b_{gh}(g,h)\right)$$

Além disso, $(w \circ f^*)\left(\left(\sum_{g\in G} a_g g\right) \otimes \left(\sum_{h\in H} b_h h\right)\right) = w\left(\sum_{\substack{g\in G\\ h\in H}} a_g b_h(g,h)\right) =$

$\sum_{\substack{g\in G\\ h\in H}} a_g b_h(g \otimes h) = \sum_{g\in G} a_g \left(\sum_{h\in H} b_h(g \otimes h)\right) = \sum_{g\in G} a_g \left(g \otimes \sum_{h\in H} b_h h\right) = \sum_{g\in G} a_g g \otimes$

$\sum_{h\in H} b_h h$. Por outro lado, $(f^* \circ w)\left(\sum_{\substack{g\in G\\ h\in H}} r_{gh}(g,h)\right) = f^*\left(\sum_{\substack{g\in G\\ h\in H}} r_{gh}(g \otimes h)\right) =$

$\sum_{\substack{g\in G\\ h\in H}} r_{gh}(g,h)$. Portanto f^* é um isomorfismo, que demonstra a proposição.

□

Definição 1.3.6. *O homomorfismo $\epsilon : RG \longrightarrow R$ dado por*

$$\epsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g$$

é chamado aplicação de aumento de RG e seu núcleo, denotado por $\triangle(G)$, é chamado de ideal de aumento de RG.

Note que, se um elemento $\alpha = \sum_{g\in G} a_g g$ pertence a $\triangle(G)$, então $\epsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g = 0$. Assim, escrevemos α da forma:

$$\alpha = \sum_{g\in G} a_g g - \sum_{g\in G} a_g = \sum_{g\in G} a_g(g-1).$$

Como os elementos da forma $g-1$, $g \in G$, pertencem a $\triangle(G)$, então $\{g-1; g \in G, g \neq 1\}$ é um conjunto de geradores de $\triangle(G)$ sobre R. Além disso, esse conjunto é linearmente independente, pois,

$\sum_{\substack{g\in G\\ g\neq 1}} a_g(g-1) = 0 \Rightarrow \sum_{\substack{g\in G\\ g\neq 1}} a_g g = \sum_{\substack{g\in G\\ g\neq 1}} a_g$, isto é, $a_{g_1}g_1 + a_{g_2}g_2 + \cdots + a_{g_r}g_r = (a_{g_1} + a_{g_2} + \cdots + a_{g_r})$.1. Mas, $\sum_{g\in G} a_g g = \sum_{g\in G} b_g g \Leftrightarrow a_g = b_g$ para $g \in G$. Assim, $a_{g_1} = \cdots = a_{g_r} = 0$. Portanto $\{g-1; g \in G, g \neq 1\}$ é linearmente independente sobre R. Com isso, mostramos que o conjunto $\{g-1; g \in G, g \neq 1\}$ é uma base de $\triangle(G)$ sobre R.

Assim, escrevemos $\triangle(G) = \left\{ \sum_{g\in G} a_g(g-1) : g \in G, g \neq 1, a_g \in R \right\}$. Se R é comutativo e G é finito, então $\triangle(G)$ é um R-módulo livre de posto $|G|-1$.

Observe também que ϵ é um epimorfismo de anéis. Logo, pelo Teorema 1.1.22 temos que $\dfrac{RG}{\triangle(G)} \simeq R$.

Capítulo 2

Semissimplicidade e o Teorema de Maschke

2.1 Semissimplicidade

Nesta seção, determinaremos condições necessárias e suficientes sobre o anel R e o grupo G para que o anel de grupo RG seja semissimples. Todo o conteúdo apresentado nesta seção encontra-se basicamente em [5] .

Definição 2.1.1. *Um submódulo N de um R-módulo M é um somando direto se existe outro R-submódulo N' de M tal que $M = N \oplus N'$.*

No caso de módulos sobre um anel arbitrário, em geral, nem todo submódulo é um somando direto. Por exemplo, $n\mathbb{Z}$, com $n \in \mathbb{Z}$, não é um somando direto de $\mathbb{Z}$ como $\mathbb{Z}$-módulo, pois para todo $m \in \mathbb{Z}$, temos $m\mathbb{Z} \cap n\mathbb{Z} = mmc(m,n)\mathbb{Z}$. Estaremos particularmente interessados em módulos que tenham essa propriedade.

Definição 2.1.2. *Um R-módulo M é chamado semissimples se todo R-submódulo de M é um somando direto.*

Todo R-módulo $M \neq \{0\}$, contém pelo menos dois submódulos, a saber M e $\{0\}$. Esses submódulos são chamados R-submódulos triviais. Um submódulo diferente desses é chamado de submódulo próprio. Um R-módulo não-trivial que não contém submódulos próprios é chamado simples.

Exemplo 2.1.3. *Seja V um espaço vetorial finitamente gerado sobre um corpo K. Então V é um K-módulo semissimples. De fato, se W é um subespaço próprio de V, então, tomando uma base de W e completando a uma base de V, é possível verificar que W é um somando direto de V.*

O lema a seguir será muito importante na demonstração dos próximos resultados.

Lema 2.1.4. *(Zorn) Seja $\mathcal{F}$ uma coleção não vazia de subconjuntos de um dado conjunto. Se toda família totalmente ordenada de elementos de $\mathcal{F}$ tem uma cota superior (em $\mathcal{F}$), então $\mathcal{F}$ contém um elemento maximal.*

Proposição 2.1.5. *Seja $N \neq \{0\}$ um submódulo de um R-módulo semissimples M. Então N é semissimples e contém um submódulo simples.*

Demonstração. Primeiramente, provemos que N é semissimples. Seja N' um submódulo arbitrário de N. Então N' também é um submódulo de M e, assim, existe outro submódulo S tal que $M = N' \oplus S$. Afirmamos que $N = N' \oplus (S \cap N)$. De fato, $N' \cap (S \cap N) \subset N' \cap S = \{0\}$. Por outro lado, dado um elemento $n \in N$, escrevemos $n = n' + s$ com $n' \in N'$ e $s \in S$. Mas $s = n - n' \in N$, assim $s \in S \cap N$.

Provemos agora que N contém um submódulo simples. Se N é simples, acabou. Suponha que N não é simples e escolha um elemento $x \in N$, $x \neq 0$. A família $\mathcal{F}$ de todos os submódulos de N que não contém x é não vazia, pois, dado N_i um submódulo de N que contém x, como N é semissimples,

existe N_j submódulo de N tal que $N = N_i \oplus N_j$. Como $x \in N_i$, $N_i \cap N_j = \{0\}$ e $x \neq 0$ então $x \notin N_j$ e, portanto, N_j está nessa família de submódulos que não contém x. Diremos que $N_i \prec N_j$ se, e somente se, $N_i \subset N_j$.

Seja $\mathcal{J} = \{N_y : y \in \mathbb{N}\}$ uma subfamília qualquer $\mathcal{F}$. Tome N^* o submódulo de N gerado pela união dos submódulos de $\mathcal{J}$. Como $x \notin N_l, \forall l \in \mathbb{N}$, $x \notin N^*$. Portanto, esta subfamília admite uma cota superior. Verificada as hipóteses do Lema de Zorn, concluímos que existe um elemento maximal N_m nesta família.

Como N é semissimples, existe um outro submódulo N_l de N tal que $N = N_m \oplus N_l$. Nosso argumento estará completo se mostrarmos que N_l é simples. Note que $x \in N_l$.

Se N_l não é simples, ele contém um submódulo próprio W e existe W' tal que $N_l = W \oplus W'$. Observe que $x \in W$ ou $x \in W'$, $N = N_m \oplus W \oplus W'$ e $N_m = (N_m + W) \cap (N_m + W')$. Como $x \notin N_m$, temos que ou $x \notin N_m + W$ ou $x \notin N_m + W'$, contradizendo a maximalidade de N_m. Portanto, N_l é simples. □

Teorema 2.1.6. *Seja M um R-módulo. Então, as seguintes condições são equivalentes:*

(i) M é semissimples;

(ii) M é uma soma direta de submódulos simples;

(iii) M é uma soma (não necessariamente direta) de submódulos simples.

Demonstração. ((iii) ⇒ (i)) Assuma que $M = \sum_{i \in I} M_i$, onde cada submódulo M_i, $i \in I$ é simples. Seja N um submódulo próprio de M arbitrário. Provemos que N é um somando direto.

Consideremos a família

$$\mathcal{J} = \left\{ \sum_{i\in J} M_i : J \subset I, \left(\sum_{i\in J} M_i \right) \cap N = \{0\} \right\}.$$

A família $\mathcal{J}$ é não vazia. De fato, como N é submódulo próprio de M, existe pelo menos um submódulo $M_j \subset M$ tal que $M_j \nsubseteq N$. Como M_j é simples, $N \cap M_j = \{0\}$ ou M_j. Se $N \cap M_j = M_j$, então $M_j \subset N$. Como $j \in I$ é qualquer, temos que $M_j \subset N$, $\forall j \in I$. Assim, $\sum_{j\in I} M_j \subset N$, o que implica $M \subset N$. Absurdo, pois, N é um submódulo próprio de M. Portanto, $N \cap M_j = \{0\}$ e $\mathcal{J}$ é não vazia.

Definimos uma ordem parcial em $\mathcal{J}$ como segue: dado dois elementos $\sum_{i\in J} M_i$ e $\sum_{w\in W} M_w$ em $\mathcal{J}$, dizemos que

$$\sum_{i\in J} M_i \prec \sum_{w\in W} M_w \text{ se, e somente se, } J \subset W.$$

Assim $(\mathcal{J}, \prec)$ satisfaz as condições do Lema de Zorn. Portanto, temos um submódulo maximal em $\mathcal{J}$, digamos $M_0 = \sum_{i\in J_0} M_i$.

Como $\left(\sum_{i\in J_0} M_i \right) \cap N = \{0\}$, o teorema estará provado se mostrarmos que $M = N + M_0$.

Se, para todo $i \in I$, temos que $M_i \subset M_0 + N$, então necessariamente $M = M_0 + N$ e a afirmação estará provada.

Assuma, por contradição, que $M \neq M_0 + N$. Logo, existe um índice $i_0 \in I$ tal que $M_{i_0} \nsubseteq M_0 + N$. Como M_{i_0} é simples, $M_{i_0} \cap (M_0 + N) = \{0\}$ ou M_{i_0}. Se $M_{i_0} \cap (M_0 + N) = M_{i_0}$, temos que $M_{i_0} \subset M_0 + N$. Absurdo, pois, estamos supondo que $M_{i_0} \nsubseteq M_0 + N$. Assim, $M_{i_0} \cap (M_0 + N) = \{0\}$.

Além disso $(M_{i_0} + M_0) \cap N = \{0\}$. De fato, temos que $(M_{i_0} + M_0) \cap N \subset (M_0 \cap M_{i_0}) + (M_{i_0} \cap N)$.

Observe que $M_0 \cap M_{i_0} = \{0\}$ ou M_{i_0}. Se $M_0 \cap M_{i_0} = M_{i_0}$, então $M_{i_0} \subset M_0$, o que implica $M_{i_0} \subset M_0 + N$, absurdo. Assim $M_0 \cap M_{i_0} = \{0\}$.

Por outro lado, $M_{i_0} \cap N = \{0\}$ ou M_{i_0}, pois M_{i_0} é simples. Se $M_{i_0} \cap N = M_{i_0}$, temos que $M_{i_0} \subset N$, o que implica $M_{i_0} \subset M_0 + N$, absurdo. Portanto

$M_{i_0} \cap N = \{0\}$.

Como $(M_{i_0} + M_0) \cap N \subset (M_0 \cap M_{i_0}) + (M_{i_0} \cap N) = \{0\}$, temos que $(M_{i_0} + M_0) \cap N = \{0\}$, o que implica $M_{i_0} + M_0 \in \mathcal{J}$. Absurdo, pois contraria a maximalidade de M_0. Portanto $M = M_0 + N$ e, como esta soma é direta, concluímos que M é um R-módulo semissimples.

((ii) $\Rightarrow$ (iii)) Trivial.

((i) $\Rightarrow$ (ii)) Suponha que M seja um R-módulo semissimples. Se M é simples, acabou. Suponha que M não é simples e seja Γ a coleção de todos os submódulos de M que podem ser escritos como uma soma direta de submódulos simples. Esses submódulos simples de M existem pela Proposição 2.1.5. Logo Γ é não vazia. Dados dois elementos $\oplus_{i\in I} M_i$ e $\oplus_{i\in J} M_j$ em Γ, dizemos que $\oplus_{i\in I} M_i \prec \oplus_{i\in J} M_i$ se, e somente se, $I \subset J$.

$(\Gamma, \prec)$ satisfaz as condições do Lema de Zorn. Logo, existe um elemento maximal M_0 em Γ, que pode ser escrito da forma $M_0 = \oplus_{i\in I} M_i$ com M_i simples, $i \in I$. A aplicação será provada se mostrarmos que $M_0 = M$.

Assuma que $M_0 \neq M$. Então, existe um submódulo N de M tal que $M = M_0 \oplus N$. Além disso, pela Proposição 2.1.5, N contém um submódulo simples S e, como N é semissimples, existe um submódulo N' de N tal que $N = S \oplus N'$. Mas então $M_0 \oplus S = \oplus_{i\in I} M_i \oplus S \supset M_0$, contradizendo a maximalidade de M_0. Isto prova o teorema. □

Se conhecermos a decomposição de um módulo como uma soma direta de submódulos simples, determinamos a estrutura de todos os submódulos.

Corolário 2.1.7. *Seja $M = \oplus_{i\in I} M_i$ uma decomposição de um módulo semissimples como uma soma direta de submódulos simples e seja N um submódulo de M. Então, existe um subconjunto de índices $J \subset I$ tal que $N \simeq \oplus_{i\in J} M_i$.*

Corolário 2.1.8. *Se M é semissimples, então para todo submódulo N de M, M/N é semissimples.*

Esse corolário mostra que o quociente de um módulo semissimples também é semissimples.

Definição 2.1.9. *Um anel R é chamado semissimples se o R-módulo ${}_RR$ é semissimples.*

Recorde que os R-submódulos de ${}_RR$ são os ideais à esquerda do anel R. Segue que R é semissimples se, e somente se, todo ideal à esquerda é um somando direto.

Seja R um anel. Dizemos que R é simples se os únicos ideais bilaterais são os triviais. Dizemos que $I \neq \{0\}$ é um ideal minimal à esquerda de R se não contiver estritamente nenhum ideal à esquerda não nulo de R, isto é, se J é um ideal à esquerda de R tal que $\{0\} \subseteq J \subseteq I$, então, $J = \{0\}$ ou $J = I$.

Proposição 2.1.10. *Seja R um anel. Todo R-módulo M é a imagem epimórfica de um R-módulo livre.*

Demonstração. Seja M um R-módulo e $\{m_i\}_{i\in I}$ um conjunto de geradores de M. Considere N o R-módulo livre que possui como base $E = \{n_i\}_{i\in I}$.

Defina

$$\begin{aligned} f : E &\longrightarrow M \\ n_i &\longmapsto m_i. \end{aligned}$$

A aplicação f é bijetora por definição. Estendendo f linearmente, obtemos o R-homomorfismo $\overline{f} : N \longrightarrow M$ tal que $\overline{f}(n) = \sum_{i\in I} r_i f(n_i)$. Dado $m \in M$, existe $(r_i)_{i\in I} \subset R$, uma sequência quase nula, tal que $m = \sum_{i\in I} r_i m_i$. Assim, $m = \sum_{i\in I} r_i m_i = \sum_{i\in I} r_i f(n_i) = \overline{f}\left(\sum_{i\in I} r_i n_i\right)$. Portanto f é sobrejetora e consequentemente um epimorfismo. □

O próximo teorema determina a estrutura de anéis semissimples.

Teorema 2.1.11. *Seja R um anel. As seguintes condições são equivalentes.*

(i) Todo R-módulo é semissimples;

(ii) R é um anel semissimples;

(iii) R é uma soma direta de um número finito de ideais minimais à esquerda.

Demonstração. $((i) \Rightarrow (ii))$ Se todo R-módulo é semissimples, por definição, temos que R é um anel semissimples.

$((ii) \Rightarrow (iii))$ Suponha que R é um anel semissimples. Por definição, ${}_RR$ é semissimples, logo $R = \oplus_{i\in I} R_i$, onde cada R_i é um submódulo simples. Como os submódulos simples de ${}_RR$ são os ideais minimais à esquerda de R, temos que cada R_i, $i \in I$, é um ideal minimal à esquerda. Portanto, para provar a implicação, basta mostrar que a soma é finita.

Em particular, o elemento $1 \in R$ pode ser escrito como uma soma finita, $1 = x_{i_1} + x_{i_2} + \cdots + x_{i_n}$, com $x_{i_j} \in R_{i_j}$. Então, para um elemento arbitrário $r \in R$, temos $r = r1 = rx_{i_1} + rx_{i_2} + \cdots + rx_{i_n}$, onde $rx_{i_j} \in R_{i_j}$, $i_j \in I$, $1 \leq j \leq n$. Assim, mostramos que $R \subset R_{i_1} + R_{i_2} + \cdots + R_{i_n}$ e, consequentemente, $R = \oplus_{j=1}^{n} R_{i_j}$, pois $R_{i_j} \subset R$, $i_j \in I$, $1 \leq j \leq n$.

$((iii) \Rightarrow (ii))$ Suponha que $R = \oplus_{i=1}^{n} R_i$ onde $R_i's$ são ideais minimais à esquerda de R. Se mostrarmos que os ideais $R_i's$ são simples então R será uma soma direta de ideais simples à esquerda, ou equivalentemente, ${}_RR$ é uma soma direta de R-submódulos simples e consequentemente R será um anel semissimples.

Suponha que exista um índice $j \in \{1. \ldots, n\}$ tal que R_j não é um ideal simples à esquerda de R. Logo R_j admite ideais à esquerda não triviais. Seja I um ideal à esquerda de R_j não trivial.

Dado $x \in R$, temos que $x = r_1 + r_2 + \cdots + r_j + \cdots + r_n$, com $r_i \in R_i, i = 1, \ldots, n$. Daí, dado $a \in I$, temos que $xa = r_1a + r_2a + \cdots + r_ja + \cdots + r_ta$. Além disso, $r_ia \in R_j$, para $1 \leq i \leq n$. Como $r_ja \in R_j$ e $xa \in R_j$, temos que $xa - r_ja \in R_j$ e, assim, $r_1a + r_2a + \cdots + \widehat{r_ja} + \cdots + r_na \in R_j \cap (\oplus_{i=1, i\neq j}^{t} R_i)$. Logo, $r_1a + r_2a + \cdots + \widehat{r_ja} + \cdots + r_na = 0$, pois a soma é direta, e obtemos $xa = r_ja$.

Como I é um ideal à esquerda de R_j, temos que $r_ja \in I$ e, pela última igualdade, $xa \in I$. Com isso, I também é um ideal à esquerda de R, contradição, pois, pela definição de ideais minimais, R_j não contém propriamente ideais à esquerda de R. Portanto cada R_i é um ideal à esquerda simples de R para $1 \leq i \leq n$. Assim, temos uma soma finita de ideais simples, consequentemente R é um anel semissimples.

$((ii) \Rightarrow (i))$ Assuma que R é um anel semissimples e seja M um R-módulo qualquer. Pela Proposição 2.1.10, $M \simeq F/K$, onde F é um R-módulo livre. Seja $\{a_i\}_{i\in I}$ uma R-base de F. Sejam $R^{(I)} = \oplus_{i\in I} R_i$, com $R_i \simeq R$, e $(r_i)_{i\in I}$ uma sequência quase-nula de $R^{(I)}$. Defina $\varphi : R^{(I)} \longrightarrow F$ por $\varphi((r_i)_{i\in I}) = \sum_{i\in I} r_ia_i$. A aplicação φ é um R-isomorfismo. Assim $F \simeq R^{(I)}$ e F é semissimples, pois R é semissimples. Logo, pelo Corolário 2.1.8, F/K é semissimples e portanto M é semissimples.

□

Exemplo 2.1.12. *Seja $M_n(D)$ o anel de matrizes $n \times n$ sobre um anel de divisão D. Mostremos que $M_n(D)$ é um anel semissimples. De fato, seja L_j o ideal à esquerda de $M_n(D)$ gerado por $\{e_{ij}, i = 1, \ldots, n\}$, onde e_{ij} denotam as matrizes unitárias usuais. Cada L_j é um ideal simples à esquerda de $M_n(D)$ e $M_n(D) = L_1 \oplus L_2 \oplus \cdots \oplus L_n$. Portanto, $M_n(D)$ é semissimples.*

Definição 2.1.13. *Um elemento e no anel R é idempotente se $e^2 = e$.*

Claramente, 0 e 1 são elementos idempotentes em todo anel R. Um idempotente diferente desses é chamado não trivial.

Teorema 2.1.14. *Um anel R é semissimples se, e somente se, todo ideal à esquerda L de R é da forma $L = Re$, onde $e \in R$ é um idempotente.*

Demonstração. Suponha que R é semissimples e seja L um ideal à esquerda de R. Então L é um somando direto. Assim, existe um ideal à esquerda L' de R tal que $R = L \oplus L'$. Escreva $1 = x + y$ com $x \in L$, $y \in L'$. Então $x = x1 = xx + xy$, o que implica $xy = x - x^2$. Note que $xy \in L'$, pois L' é um ideal a esquerda de R e $x - x^2 \in L$ pois $x \in L$. Como $L \cap L' = \{0\}$, segue que $xy = 0$. Assim, $x = x^2$ é idempotente. Analogamente, mostra-se que L' admite um elemento idempotente. Temos que $Rx \subseteq L$, pois L é um ideal à esquerda de R. Agora, dado $a \in L$, temos que $a = a1 = a(x + y) = ax + ay$, o que implica $ay = a - ax$ e consequentemente $ay \in L' \cap L = \{0\}$. Como $a = ax \in Rx$, temos que $L \subseteq Rx$ e portanto $L = Rx$.

Reciprocamente, assuma que os ideais a esquerda L de R são da forma $L = Re$, onde $e \in R$ é idempotente. Provemos que L é um somando direto. Considere o ideal $L' = R(1 - e)$. Dado um elemento $x \in R$, sempre podemos escrever $x = xe + x(1 - e)$ e assim temos que $R = Re + R(1 - e)$. Além disso, se $x \in Re \cap R(1 - e)$, temos que $x = re = s(1 - e)$, para alguns r, $s \in R$. Então $xe = ree = re^2 = re = x$. Por outro lado, temos que $xe = s(1 - e)e = 0$, logo $x = xe = 0$ e segue que $Re \cap R(1 - e) = 0$. Portanto $R = Re \oplus R(1 - e)$ e Re é um somando direto.

□

Lema 2.1.15. *Sejam L um ideal minimal à esquerda de um anel semissimples R e M um R-módulo simples. Então $LM \neq \{0\}$ se, e somente se, $L \simeq M$ como R-módulos. Neste caso $LM = M$.*

Demonstração. Assuma que $LM \neq \{0\}$. Como LM é um R-submódulo de M e M é simples, segue que $LM = M$.

Agora, como $LM \neq \{0\}$, existem $l \in L$ e $m \in M$ tal que $lm \neq 0$. Consideremos o R-homomorfismo $f : L \longrightarrow M$ dado por $f(x) = xm$. Como $Lm = M$, segue que f é um epimorfismo. Temos que $Ker(f)$ é um ideal à esquerda de L e consequentemente, é um ideal à esquerda de R. Como L é minimal, temos que $Ker(f) = \{0\}$ ou L. Se $Ker(f) = L$, então $Im(f) = \{0\}$, Logo $lm = 0 \in M$, absurdo. Assim $Ker(f) = \{0\}$, f é injetora e, portanto, temos que $L \simeq M$.

Reciprocamente, assuma que $L \simeq M$ como R-módulos. Então existe um R-isomorfismo $f : L \longrightarrow M$. Como L é um ideal à esquerda de R e R é um anel semissimples, temos que existe um idempotente $e \in R$ tal que $L = Re$. Defina $m_0 = f(e)$. Daí, $m_0 = f(e) = f(e^2) = ef(e) = em_0$. Note que $m_0 \neq 0$, pois caso contrário $Ker(f) = L$ e f não seria um R-isomorfismo. Logo $em_0 \neq 0$ e, portanto, $LM \neq \{0\}$. □

Proposição 2.1.16. *Seja $R = \oplus_{i=1}^{t} L_i$ uma decomposição de um anel semissimples R como uma soma direta de ideais minimais à esquerda. Então, todo R-módulo simples é isomorfo a um dos L_i na decomposição.*

Demonstração. Seja $R = \oplus_{i=1}^{t} L_i$ uma decomposição de R como uma soma direta de ideais minimais à esquerda e seja M um R-módulo simples. Então, como $RM \neq \{0\}$ e é um submódulo de M, da simplicidade de M temos que $RM = M$. Mas $RM = \oplus_{i=1}^{t} L_i M$. Logo, existe um índice $j \in \{1, \ldots, t\}$ tal que $L_j M \neq \{0\}$ e, pelo Lema 2.1.15, temos que $L_j \simeq M$. □

A Proposição 2.1.16 diz que temos uma quantidade finita de R-módulos simples.

Voltando aos anéis de grupos, nos perguntamos: todo anel de grupo é

semissimples? A resposta é não. Como exemplo, considere o anel de grupo $\mathbb{Z}_2C_2 = \{0, 1, g, 1+g\}$. Seja $\{1+g, 0\}$ o ideal minimal à esquerda gerado por $1+g \in \mathbb{Z}_2C_2$. Não existe outro ideal minimal à esquerda J de $\mathbb{Z}_2C_2$ tal que $\mathbb{Z}_2C_2 = \langle 1+g \rangle \oplus J$. Portanto $\mathbb{Z}_2C_2$ não é semissimples. Então em quais condições um anel de grupo é semissimples? A resposta para essa pergunta aparece na próxima seção.

A seguir, demonstraremos que anéis de grupos sobre grupos infinitos não são semissimples. Uma vez que temos esse resultado, nos preocuparemos apenas quando o grupo é finito. Nesse caso, o Teorema de Maschke nos dá condições necessárias e suficientes para que o anel de um grupo finito seja semissimples.

Teorema 2.1.17. *Sejam R um anel qualquer e G um grupo. Se G tem ordem infinita, então RG não é semissimples.*

Demonstração. Se RG é semissimples, pelo Teorema 2.1.14, $\triangle(G) = RGe$, onde $e \in R$ é um idempotente. Como $\triangle(G)$ é gerado por $\{g-1 : g \in G, g \neq 1\}$ e $e(1-e) = 0$, temos que $(g-1)(1-e) = 0$ para todo $g \in G$ e $g \neq 1$. Se $f = 1 - e = \sum_{h \in G} \alpha_h h$, então $\sum_{h \in G} \alpha_h gh = \sum_{h \in G} \alpha_h h$ para todo $g \in G$ e $g \neq 1$. Se $p \in supp(f)$, pela Definição 1.3.2, $\alpha_p \neq 0$ e, consequentemente, $gp \in supp(f)$ para todo $g \in G$. Logo $G \subset supp(f)$ e assim $supp(f)$ é infinito, absurdo. Portando RG não é semissimples. □

2.2 O Teorema de Maschke

Definição 2.2.1. *Seja X um subconjunto do anel de grupo RG. O anulador à esquerda de X é o conjunto*

$$Ann_l(X) = \{\alpha \in RG : \alpha x = 0, \forall x \in X\}.$$

Analogamente, definimos o anulador a direita de X por:

$$Ann_r(X) = \{\alpha \in RG : x\alpha = 0, \forall x \in X\}$$

O conjunto $Ann_r(X)$ definido acima é um subanel de RG. Além disso, para todo $\alpha \in Ann_r(X)$, $y \in RG$ e $x \in X$ temos que $x(\alpha y) = (x\alpha)y = 0\beta = 0$, assim, $\alpha y \in Ann_r(X)$. Portanto, $Ann_r(X)$ é ideal à direita de RG. Analogamente, $Ann_l(X)$ é um ideal à esquerda de RG.

Definição 2.2.2. *Dado um anel de grupo RG e um subconjunto finito $X \neq \emptyset$ do grupo G, denotaremos por $\widehat{X}$ o seguinte elemento de RG:*

$$\widehat{X} = \sum_{x \in X} x.$$

Lema 2.2.3. *Temos que $Ann_r(\triangle(G)) \neq \{0\}$ se, somente se, G é finito. Nesse caso, $Ann_r(\triangle(G)) = \widehat{G}RG$. Além disso, o elemento $\widehat{G}$ é central em RG e $Ann_r(\triangle(G)) = Ann_l(\triangle(G)) = RG\widehat{G}$.*

Demonstração. Assuma que $Ann_r(\triangle(G)) \neq \{0\}$ e seja $\alpha = \sum_{g \in G} a_g g \in Ann_r(\triangle(G))$ não nulo. Para cada elemento $h \in G$, $h \neq 1$, temos $(h-1)\alpha = 0$ e consequentemente, $h\alpha = \alpha$. Assim, $\alpha = \sum_{g \in G} \alpha_g g = \sum_{g \in G} \alpha_g hg$. Tome $g_0 \in supp(\alpha)$. Então $\alpha_{g_0} \neq 0$ e $hg_0 \in supp(\alpha)$ para todo $h \in G$. Uma vez que o $supp(\alpha)$ é finito, temos que G é finito.

Reciprocamente, assuma que G é finito. Consideremos $G = \{1 = g_1, g_2, \ldots g_t\}$ e provemos que $Ann_r(\triangle(G)) \neq 0$. Se G é finito, $g\widehat{G} = \widehat{G}$, $\forall\ g \in G$, pois $gg_j \in G$, para todo $j = 1, \ldots, n$. Assim, $(g-1)\widehat{G} = 0$, $\widehat{G} \in Ann_r(\triangle(G))$ e concluímos que $Ann_r(\triangle(G)) \neq 0$ e $\widehat{G}RG \subseteq Ann_r(\triangle(G))$.

Para concluir a primeira igualdade da proposição, provemos que

$$Ann_r(\triangle(G)) \subseteq \widehat{G}RG.$$

Tome $\alpha \in Ann_r(\triangle(G))$, $\alpha \neq 0$, e considere $G = \{1, g_1, g_2, \ldots, g_t\}$. Como $\triangle(G)$ é gerado por $g - 1, g \in G$, $g \neq 1$, temos que $(g_j - 1)\alpha = 0$, $\forall\ j = 1$, ..., t, ou seja, $g_j\alpha = \alpha$, $\forall\ j = 1, \ldots, t$.

Se $\alpha = \sum_{i=1}^{r} a_{g_i} g_i$, $g_i \in supp(\alpha)$, $i = 1, \ldots, r$, então $\sum_{i=1}^{r} a_{g_i} g_j g_i = \sum_{i=1}^{r} a_{g_i} g_i$.

Como $g_j \neq 1, \forall j = 1, \ldots, t$, temos $g_j g_i \in supp(\alpha), \forall i = 1, \ldots, r$, $j = 1, \ldots, t$, e o coeficiente de g_i é igual ao coeficiente $g_j g_i, \forall i, j$. Assim,

$$supp(\alpha) = \{g_j g_i : 1 \leq j \leq t, 1 \leq i \leq r\}.$$

Reescrevendo α, temos:

$\alpha = \sum_{i=1}^{r} a_{g_i} g_i + a_{g_1} + \sum_{j=1}^{t} g_j g_1 + a_{g_2} \sum_{j=1}^{t} g_j g_2 + \cdots + a_{g_r} \sum_{j=1}^{t} g_j g_r = a_{g_1} \widehat{G} g_1 + a_{g_2} \widehat{G} g_2 + \cdots + a_{g_r} \widehat{G} g_r = \widehat{G}\beta, \beta \in RG$. Portanto, $Ann_r(\triangle(G)) = \widehat{G}RG$.

Agora, $g^{-1}\widehat{G}g = g^{-1}\left(\sum_{x \in G} x\right)g = \sum_{x \in G} g^{-1}xg = \sum_{y \in G} y = \widehat{G}$, $\forall g \in G$. Logo $\widehat{G}g = g\widehat{G}$ para todo $g \in G$, que mostra que $\widehat{G}$ está no centro de RG. Consequentemente $RG\widehat{G} = \widehat{G}RG$ e segue o resultado. □

Corolário 2.2.4. *Seja G um grupo finito. Então:*

(i) $Ann_l(\triangle(G)) = R\widehat{G}$, *onde* $R\widehat{G} := \{a\widehat{G} : a \in R\}$.

(ii) $Ann_r(\triangle(G)) \cap \triangle(G) = \{a\widehat{G} : a \in R, a|G| = 0\}$

Demonstração. (i) Dado $x \in RG\widehat{G}$, existe $\alpha \in RG$ tal que $x = \alpha\widehat{G}$. Se $\alpha = \sum_{g \in G} a_g g$ com $a_g \in R$, temos $x = \left(\sum_{g \in G} a_g g\right)\widehat{G} = \sum_{g \in G} a_g(g\widehat{G}) = \sum_{g \in G} a_g(\widehat{G}) = \left(\sum_{g \in G} a_g\right)\widehat{G}$. Assim, $RG\widehat{G} \subseteq R\widehat{G}$. Como $R \subset RG$ segue $R\widehat{G} \subseteq RG\widehat{G}$.
(ii) Dado $x \in Ann_r(\triangle(G)) \cap \triangle(G)$ temos que $\epsilon(x) = \epsilon(a\widehat{G}) = a\epsilon(\widehat{G}) = a|G| = 0$. Portanto segue o resultado. □

Lema 2.2.5. *Seja I um ideal bilateral de um anel R. Suponha que exista um ideal à esquerda J de R tal que $R = I \oplus J$ (como R-módulos à esquerda). Então $J \subset Ann_r(I)$.*

Demonstração. Dados $x \in I$ e $y \in J$, temos que $xy \in I \cap J$, pois I é um ideal bilateral e J é um ideal à esquerda de R. Como $I \cap J = \{0\}$, segue que $xy = 0$ e $y \in Ann_r(I)$. Portanto $J \subset Ann_r(I)$. □

Lema 2.2.6. *Se o ideal de aumento $\triangle(G)$ é um somando direto de RG, como RG-módulo, então G é finito e $|G|$ é invertível em R.*

Demonstração. Assuma que $\triangle(G)$ é um somando direto de RG, então $RG = \triangle(G) \oplus J$. Como $RG \neq \triangle(G)$, pois $\epsilon(g) = 1$, $\forall g \in G$ então $J \neq \{0\}$. Deste modo, pelo Lema 2.2.5, $Ann_r(\triangle(G)) \neq \{0\}$ e, pelo Lema 2.2.3, G é finito.

Escreva $1 = e_1 + e_2$ com $e_1 \in \triangle(G)$ e $e_2 \in J$. Então $1 = \epsilon(1) = \epsilon(e_1) + \epsilon(e_2) = \epsilon(e_2)$. Pelo Lema 2.2.5, $e_2 \in Ann_l(\triangle(G))$ e pelo Corolário 2.2.4, $e_2 = a\widehat{G}$, para algum $a \in R$. Logo, $1 = \epsilon(e_2) = \epsilon(a\widehat{G}) = a\epsilon(\widehat{G}) = a|G|$ com $a \in R$. Portanto $|G|$ é invertível em R. □

Definição 2.2.7. *Sejam M um R-módulo e N um submódulo de M. Um R-homomorfismo $\pi : M \longrightarrow M$ é chamado de projeção sobre N se $Im(\pi) = N$ e $\pi(n) = n$ para cada $n \in N$.*

No próximo resultado iremos caracterizar os R-homomorfismo que são projeções. Mas antes, observamos que se $T : M \longrightarrow M$ é R-homomorfismo, então podemos decompor M como sendo a soma $N_1 + N_2$ onde $N_1 = Im(T)$ e $N_2 = Im(Id_M - T)$. De fato, cada elemento $m \in M$ pode ser escrito como $m = T(m) + (m - T(m)) = T(m) + (Id_M - T)(m)$, o que prova nossa afirmação. Em geral, esta soma não tem por que ser direta como nos mostra o seguinte exemplo. Considere o R-homomorfismo $T : R^2 \longrightarrow R^2$ dado por $T(x, y) = (x + y, y)$. Observe que $Im(T) \cap Im(Id_M - T) = \langle(1, 0)\rangle \neq \{0\}$. Na realidade, a soma $N_1 + N_2$ como acima será direta se, e somente se, T for uma projeção sobre N_1.

Proposição 2.2.8. *Seja $\pi : M \longrightarrow M$ um R-homomorfismo e escreva $M = N_1 + N_2$ onde $N_1 = Im(\pi)$ e $N_2 = Im(Id_M - \pi)$. As seguintes afirmações são equivalentes:*

(i) π é uma projeção sobre N_1;

(ii) $\pi^2 = \pi$;

(iii) $N_1 \cap N_2 = \{0\}$.

Demonstração. $((i) \Rightarrow (ii))$ Suponha que π seja uma projeção sobre N_1 e seja $m \in M$. Se escrevermos $\pi(m) = n$, então $\pi(\pi(m)) = \pi(n) = n = \pi(m)$ e $\pi^2 = \pi$, como queríamos.

$((ii) \Rightarrow (iii))$ Seja $n \in N_1 \cap N_2$. Como $n \in N_1$, então existe $m \in M$ tal que $\pi(m) = n$. Usando o fato de que $\pi^2 = \pi$, teremos que $\pi(n) = \pi(\pi(m)) = \pi(m) = n$. Por outro lado, como $n \in N_2$, temos que existe $m' \in M$ tal que $n = m' - \pi(m')$. Com isto, segue que $n = \pi(n) = \pi(m') - \pi(\pi(m')) = \pi(m') - \pi^2(m') = 0$ e $N_1 \cap N_2 = \{0\}$.

$((iii) \Rightarrow (i))$ Assuma que $N_1 \cap N_2 = \{0\}$, como $M = N_1 + N_2$ temos que $M = N_1 \oplus N_2$. Dado $n_1 \in N_1 \subset M$, podemos escrever $n_1 = \pi(n_1) + (Id_M - \pi)(n_1)$. Como $M = N_1 \oplus N_2$, então, todo elemento em M é escrito de maneira única, por isso, temos que $\pi(n_1) = n_1$ e $(id_M - \pi)(n_1) = 0$. Como $N_1 = Im(\pi)$, concluímos que π é uma projeção de N_1. □

Corolário 2.2.9. *Seja $\pi : M \longrightarrow M$ uma projeção sobre $Im(\pi)$. Então o submódulo $Im(Id_M - \pi)$ é o núcleo de π.*

Demonstração. Considerando $n = (Id_M - \pi)(m)$, teremos então que $\pi(n) = (\pi - \pi^2)(n) = \pi(n) - \pi^2(n) = 0$, e consequentemente, $(Id_M - \pi)(M) \subseteq Ker(\pi)$. Reciprocamente, se $\pi(n) = 0$, como $n = \pi(n) + (Id_M - \pi)(n)$, segue que $n = (Id_M - \pi)(n)$, isto é, n pertence a $(Id_M - \pi)(M)$. Portanto, $Ker(\pi) = (Id_M - \pi)(M)$. □

Agora, estamos em condições de demonstrar o principal teorema deste capítulo, o Teorema de Maschke (1898-99), que nos dá condições necessárias e suficientes sobre o anel R e o grupo G para que o anel de grupo RG seja semissimples.

Teorema 2.2.10 (Teorema de Maschke)**.** *Seja G um grupo. Então, o anel de grupo RG é semissimples se, e somente se, satisfaz as seguintes condições:*

(i) R é um anel semissimples;

(ii) G é finito;

(iii) $|G|$ é invertível em R.

Demonstração. Assuma que RG é semissimples e seja $\triangle(G)$ o ideal de aumento. Sabemos que $\dfrac{RG}{\triangle(G)} \simeq R$ e, pelo Corolário 2.1.8, $\dfrac{RG}{\triangle(G)}$ é semissimples. Consequentemente, R é semissimples. Como a semissimplicidade de RG implica que $\triangle(G)$ é um somando direto, temos que, pelo Lema 2.2.6, as condições (ii) e (iii) são satisfeitas.

Reciprocamente, assuma que as condições (i), (ii) e (iii) são satisfeitas e seja M um RG-submódulo de RG. Como R é semissimples, pelo Teorema 2.1.11, todo R-módulo é semissimples. Como RG é um R-módulo, temos que RG é semissimples como R-módulo. Logo, existe um R-submódulo N de RG tal que $RG = M \oplus N$. Seja $\pi : RG \longrightarrow M$ a projeção canônica associada à soma direta. Defina $\pi^* : RG \longrightarrow M$ por $\pi^*(x) = \frac{1}{|G|} \sum\limits_{g \in G} g^{-1}\pi(gx)$.

Se provarmos que π^* é na verdade um RG-homomorfismo tal que π^* é uma projeção sobre M, então, pela Proposição 2.2.8, RG será semissimples e $RG = M \oplus Im(Id_M - \pi^*)$, onde $Im(Id_M - \pi^*) = Ker(\pi^*)$.

Como π é um R-homomorfismo de anéis, temos que $\pi^*(\alpha + \beta) = \pi^*(\alpha) + \pi^*(\beta)$, $\pi^*(\alpha\beta) = \pi^*(\alpha)\pi^*(\beta)$ e $\pi^*(r\alpha) = r\pi^*(\alpha)$ para todo α, $\beta \in RG$ e

$r \in R$. Assim, para concluir que π^* é um RG-homomorfismo, mostremos que $\pi^*(hx) = h\pi^*(x)$ para todo $h \in G$ e para todo $x \in G$. Temos que

$$\pi^*(hx) = \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(ghx) = \frac{h}{|G|}\sum_{g\in G}(gh)^{-1}\pi((gh)x) = h\pi^*(x),$$

pois, como G é finito, gh continua sendo um termo do somatório.

Agora, $\pi^*(m) = m$, para todo $m \in M$. De fato, como M é um RG-módulo, temos que $gm \in M$, para todo $g \in G$. Assim,

$$\pi^*(m) = \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(gm) = \frac{1}{|G|}\sum_{g\in G} g^{-1}(gm) = \frac{1}{|G|}\sum_{g\in G} m = \frac{1}{|G|}|G|m = m.$$

Isto mostra também que $M \subset Im(\pi^*)$ e, assim, $M = Im(\pi^*)$. Portanto, π^* é uma projeção sobre M e $RG = M \oplus Ker(\pi^*)$, isto é, RG é semissimples, o que conclui a demonstração. □

Se R é um corpo, então R é semissimples e $|G|$ é invertível em R se, e somente se, $|G| \neq 0$ em R, isto é, se e somente se, $char(R) \nmid |G|$.

Corolário 2.2.11. *Seja G um grupo finito e seja K um corpo. Então KG é semissimples se, e somente se, $char(K) \nmid |G|$.*

2.2.1 Teorema de Wedderburn-Artin

Para dar uma caracterização mais fina da decomposição de um anel de grupo semissimples, enunciaremos o teorema de Wedderburn-Artin. Mais detalhes sobre esta subseção pode ser consultado em [5], seções 2.6 e 3.4.

Teorema 2.2.12 (Wedderburn-Artin)**.** *Um anel R é semissimples se, e somente se, é uma soma direta de álgebras de matrizes sobre anéis de divisão, isto é,*

$$R \simeq M_{n_1}(D_1) \oplus \cdots \oplus M_{n_s}(D_s).$$

Além disso, esta decomposição é única a menos de isomorfismos dos anéis de divisão e da reordenação dos índices.

Como consequência do teorema de Wedderburn-Artin temos o seguinte resultado para anéis de grupo.

Teorema 2.2.13. *Seja RG um anel de grupo semissimples. Então cada componente simples de RG é isomorfa a um anel de matrizes da forma $M_{n_i}(D_i)$, onde D_i é um anel de divisão. Em particular, se $R = K$ é um corpo, cada D_i contém uma cópia isomórfica de K em seu centro e o isomorfismo $KG \simeq \oplus_{i=1}^{r} M_{n_i}(D_i)$ é um isomorfismo de K-álgebras. Além disso, se K é algebricamente fechado, então $KG \simeq \oplus_{i=1}^{r} M_{n_i}(K)$ e $n_1^2 + n_2^2 + \cdots + n_r^2 = |G|$.*

Capítulo 3

Teorema de Perlis-Walker

3.1 Extensões de Corpos

Nesta seção apresentaremos, sem demonstração, alguns resultados sobre extensões de corpos. O leitor interessado pode encontrar as demonstrações dos resultados deste capítulo nas referências [3, 4].

Definição 3.1.1. *Um corpo F é uma extensão do corpo K se $K \subseteq F$ é um subcorpo de F.*

Se F é uma extensão do corpo K, então $1_K = 1_F$, F é um espaço vetorial sobre K e denotamos por $[F : K]$ a dimensão de F sobre K.

Exemplo 3.1.2. $\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ *é uma extensão de* $\mathbb{Q}$. *Temos que* $\{1, \sqrt{2}\}$ *é uma base de* $\mathbb{Q}(\sqrt{2})$ *sobre* $\mathbb{Q}$ *e* $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Definição 3.1.3. *Dizemos que F é uma extensão finita (infinita) de K se $[F : K]$ é finita (infinita).*

Exemplo 3.1.4. *Se p primo, então* $\mathbb{Q}(\sqrt{p}) := \{a + b\sqrt{p} : a, b \in \mathbb{Q}\}$ *é uma extensão finita de* $\mathbb{Q}$ *e* $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$.

Teorema 3.1.5. *Sejam F uma extensão do corpo E e E uma extensão do corpo K. Então $[F : K] = [F : E][E : K]$. Consequentemente, $[F : K]$ é finito se, somente se, $[F : E]$ e $[E : K]$ são finitos.*

Definição 3.1.6. *Sejam K um domínio de integridade e $f(x)$ não nulo em $K[x]$. Se o polinômio $f(x)$ não é unidade em $K[x]$, dizemos que $f(x)$ é irredutível sobre K se sempre que $f(x) = g(x)h(x)$, onde $g(x), h(x) \in K[x]$, então ou $g(x)$ ou $h(x)$ é unidade em $K[x]$. Caso $f(x) = g(x)h(x)$ e $g(x)$ e $h(x)$ não sejam unidades em $K[x]$, então dizemos que $f(x)$ é um polinômio redutível sobre K.*

Exemplo 3.1.7. *O polinômio $f(x) = 2x^2 + 4$ é irredutível sobre $\mathbb{Q}$ e $\mathbb{R}$, mas é redutível sobre $\mathbb{Z}$, pois $2x^2 + 4 = 2(x^2 + 2)$, com 2 e $x^2 + 2$ não invertíveis em $\mathbb{Z}[x]$. Note que, em $\mathbb{C}[x]$, $2x^2+4 = (\sqrt{2}x-2i)(\sqrt{2}x+2i)$. Como $\sqrt{2}x-2i$ e $\sqrt{2}x + 2i$ não são unidades em $\mathbb{C}[x]$, temos que $f(x)$ é redutível sobre $\mathbb{C}$.*

Seja K um corpo. Então $K[x]$ é um domínio de ideais principais. Além disso, dado um ideal I não nulo em $K[x]$ e $g(x)$ um elemento em $K[x]$, então $I = \langle g(x) \rangle$ se, e somente se, $g(x)$ é um polinômio não nulo de menor grau em I.

Exemplo 3.1.8. *Considere o $\mathbb{R}$-homomorfismo $\alpha : \mathbb{R}[x] \longrightarrow \mathbb{C}$ dado $f(x) = i$, $f(1) = 1$. Então $x^2 + 1 \in Ker(\alpha)$. Como as raízes desse polinômio são i e $-i$ e não estão em $\mathbb{R}$, x^2+1 é irredutível sobre $\mathbb{R}$ e, além disso, é o polinômio de menor grau em $Ker(\alpha)$. Assim, $Ker(\alpha) = \langle x^2 + 1 \rangle$ e $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ é isomorfo a $\mathbb{C}$.*

Teorema 3.1.9. *Seja K um corpo e seja $f(x)$ um polinômio não constante em $K[x]$. Então existe uma extensão F de K em que $f(x)$ tem pelo menos uma raiz.*

Exemplo 3.1.10. *Seja* $f(x) = x^5 + 2x^2 + 2x + 2 \in \mathbb{Z}_3[x]$. *Como* $x^2 + 1$ *e* $x^3 + 2x + 2$ *não possuem raízes em* $\mathbb{Z}_3$, *concluímos que ambos são irredutíveis sobre* $\mathbb{Z}_3$. *Assim, a fatoração de* $f(x)$ *sobre* $\mathbb{Z}_3$ *é* $(x^2 + 1)(x^3 + 2x + 2)$. *Portanto, uma extensão* F *de* $\mathbb{Z}_3$ *na qual* $f(x)$ *tem pelo menos uma raiz é* $F = \mathbb{Z}_3[x]/\langle x^2 + 1\rangle$.

Definição 3.1.11. *Sejam* K *um corpo e* F *uma extensão de* K. *Dizemos que um elemento* $a \in F$ *é algébrico sobre* K *se existe um polinômio* $f(x) \in K[x] - \{0\}$ *tal que* $f(a) = 0$. *Caso contrário, dizemos que* a *é transcendente sobre* K. *Denotamos por* $K(a)$ *o "menor" corpo que contém* K *e* a. *Ele é a interseção de todos os corpos que contêm* K *e* a.

Teorema 3.1.12. *Seja* $p(x) \in K[x]$ *irredutível sobre* K. *Se* a *é uma raiz de* $p(x)$ *em alguma extensão* F *de* K, *então* $K(a)$ *é isomorfo a* $K[x]/\langle p(x)\rangle$. *Além disso, se* $deg(p(x)) = n$, *então todo elemento de* $K(a)$ *é expresso unicamente na forma*

$$c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \cdots + c_1 a + c_0$$

onde c_0, c_1, ..., $c_{n-1} \in K$.

O teorema acima nos diz que $K(a)$ tem como K-base $\{1, a, \ldots, a^{n-1}\}$ e $[K(a) : K] = deg(p(x))$. Definimos $K(a_1, a_2) := K(a_1)(a_2)$ e, indutivamente, $K(a_1, \ldots, a_n) := K(a_1, \ldots, a_{n-1})(a_n)$.

Corolário 3.1.13. *Seja* $p(x) \in K[x]$ *um polinômio irredutível sobre* K. *Se* a *é uma raiz de* $p(x)$ *em alguma extensão* F *de* K *e* b *é uma raiz de* $p(x)$ *em alguma extensão* F' *de* K, *então o corpos* $K(a)$ *e* $K(b)$ *são isomorfos.*

3.1.1 Extensões Ciclotômicas

Um número complexo é uma raiz n-ésima da unidade se é raiz do polinômio $f(x) = x^n - 1$. As raízes n-ésimas da unidade são dadas por

$\zeta_k = cos(\frac{2k\pi}{n}) + isen(\frac{2k\pi}{n}), k = 0, \ldots, n-1$. As raízes n-ésimas da unidade formam um grupo cíclico multiplicativo de ordem n, gerado por $\zeta = \zeta_1$. Os geradores desse grupo são todos os elementos da forma ζ^k, onde $1 < k < n$ e $mdc(n, k) = 1$, os quais são chamados de raízes n-ésimas primitivas da unidade. Observe que, dado n, existem $\varphi(n)$ raízes n-ésimas primitivas da unidade, onde φ é a função de Euler.

Dizemos que uma raiz primitiva da unidade ζ tem ordem n se n é o menor inteiro positivo tal que $\zeta^n = 1$. Uma extensão F do corpo K é ciclotômica de ordem n, se $F = K(\zeta)$, onde ζ é uma raiz primitiva da unidade de ordem n.

O próximo resultado será importante na demonstração do Teorema de Perlis-Walker.

Teorema 3.1.14. *Seja K um corpo tal que a característica não divide ab, onde $a, b \in \mathbb{Z}_+$. Sejam ζ_a, ζ_b raízes primitivas da unidade de ordem a e b respectivamente, $m = mmc(a, b)$ e ζ_m uma raiz primitiva da unidade de ordem m. Então $K(\zeta_a, \zeta_b) = K(\zeta_m)$.*

Demonstração. Temos que $a|m$ e $b|m$. Logo as raízes primitivas da unidade de ordem a e b estão em $K(\zeta_m)$. Assim, $K(\zeta_a) \subseteq K(\zeta_m)$, $K(\zeta_b) \subseteq K(\zeta_m)$ e, consequentemente, $K(\zeta_a, \zeta_b) \subseteq K(\zeta_m)$.

Reciprocamente, observamos que $\langle\zeta_m\rangle$ é subgrupo de $\langle\zeta_a, \zeta_b\rangle$. De fato, $|\langle\zeta_a, \zeta_b\rangle|$ é múltiplo da ordem de $\langle\zeta_a\rangle$ e $\langle\zeta_b\rangle$ então, é múltiplo de m. Logo $\langle\zeta_a, \zeta_b\rangle$ contém $\langle\zeta_m\rangle$. Assim, $\zeta_m \in K(\zeta_a, \zeta_b)$ e $K(\zeta_m) \subseteq K(\zeta_a, \zeta_b)$. Portanto $K(\zeta_m) = K(\zeta_a, \zeta_b)$. □

Definição 3.1.15. *Para qualquer inteiro positivo n, sejam ζ_1, ζ_2, $\ldots, \zeta_m$ as n-ésimas raízes primitivas da unidade. Definimos o n-ésimo polinômio ciclotômico por $\Phi_n(x) = (x - \zeta_1)(x - \zeta_2)\cdots(x - \zeta_m)$.*

Note que $\Phi_n(x)$ é mônico e tem grau $\varphi(n)$.

Exemplo 3.1.16. *Por definição,* $\Phi_1(x) = x - 1$, *onde* 1 *é a única raiz de* $x - 1$. $\Phi_2(x) = x + 1$, -1 *é a raiz primitiva da unidade de ordem* 2. $\Phi_3(x) = (x - w)(x - w^2)$, *onde* $w = cos(\frac{2\pi}{3}) + isen(\frac{2\pi}{3}) = (-1 + i\sqrt{3})/2$ *é a raiz primitiva da unidade de ordem* 3, *e* $\Phi_3(x) = x^2 + x + 1$.

Teorema 3.1.17. *Para todo inteiro positivo* n, $x^n - 1 = \Pi_{d|n}\Phi_d(x)$, *onde o produto percorre todos os divisores positivos* d *de* n.

Pelo Teorema 3.1.17, se p é um primo, então $x^p - 1 = \Phi_1(x)\Phi_p(x)$. Assim $\Phi_p(x) = (x^p - 1)/(x - 1) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

Exemplo 3.1.18. *Seja* $f(x) = x^6 - 1$. *Pelo teorema anterior,* $x^6 - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x)$. *Assim,* $\Phi_6(x) = (x^6-1)/((x-1)(x+1)(x^2+x+1)) = x^2 - x + 1$.

Utilizando um argumento indutivo, é possível mostrar que os coeficientes de $\Phi_n(x)$ são inteiros.

Teorema 3.1.19. *O polinômio ciclotômico* $\Phi_n(x)$ *é irredutível sobre* $\mathbb{Z}$.

Seja E uma extensão do corpo K. Um elemento $\alpha \in E$, algébrico sobre K, diz-se separável sobre K se existe $f(x) \in K[x] - \{0\}$ tal que $f(\alpha) = 0$ e $f(x)$ não possui raízes múltiplas em nenhuma extensão de K. O corpo E diz-se separável sobre K se todos os elementos de E são separáveis sobre K.

Dado $f(x) \in K[x]$, definimos a derivada formal de f do seguinte modo: se $f(x) = \sum_{i=0}^{n} a_i x^i$, então $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$. É possível mostrar que são válidas as regras de derivação usuais $(af)' = af', (f + g)' = f' + g', (fg)' = f'g + fg'$ e $\left(\frac{f}{g}\right)' = \frac{f'g - fg'}{(g')^2}$, para todo $f, g \in K[x], a \in K$.

Teorema 3.1.20. *Seja $f(x)$ um polinômio não nulo em $K[x]$. Então f possui raízes distintas se, e somente se, f e f' não possuem raízes comuns em nenhuma extensão de K.*

Demonstração. ($\Rightarrow$) Suponha que $K \subseteq E$ e $\alpha \in E$ é tal que $f(\alpha) = 0 = f'(\alpha)$. Escreva $f(x) = (x-\alpha)g(x)$, $g(x) \in E[x]$. Temos que $f'(x) = g(x) + (x-\alpha)g'(x)$. Logo $0 = f'(\alpha) = g(\alpha)$ e $g(x) = (x-\alpha)h(x)$, $h(x) \in E[x]$. Portanto $(x-\alpha)^2 | f(x)$ e $f(x)$ não possui raízes distintas.

($\Leftarrow$) Suponha que f não possui raízes distintas. Logo, existe uma extensão $K \subseteq E$ e um elemento $\alpha \in E$ tal que $(x-\alpha)^2 | f(x)$ em $E[x]$. Logo, $f(x) = (x-\alpha)^2 h(x)$, $h(x) \in E[x]$ e $f'(x) = 2(x-\alpha)h(x) + (x-\alpha)^2 h'(x)$. Assim, $f(\alpha) = 0 = f'(\alpha)$. □

Corolário 3.1.21. *Seja $f \in K[x]$ irredutível sobre K. Então f possui raízes distintas se, e somente se, f' não é o polinômio nulo.*

Demonstração. ($\Leftarrow$) Suponha que $deg(f) = n$. Se f não possui raízes distintas, então $f(\alpha) = 0 = f'(\alpha)$ para algum $\alpha \in E \supseteq K$. Como f é irredutível, f divide todo polinômio em $K[x]$ que possui α como raiz. Logo, $f | f'$ e como $deg(f') \leq n-1$, devemos ter $f' \equiv 0$.

($\Rightarrow$) Suponha que $f' \equiv 0$. Seja $K \subseteq E$ na qual f possui alguma raiz α. Então $f(\alpha) = 0 = f'(\alpha)$ e, pelo Teorema 3.1.20, f não possui raízes distintas. □

Corolário 3.1.22. *Seja $f \in K[x]$ e assuma que f é irredutível sobre K, mas não possui raízes distintas. Então $char(K) = p > 0$ e $f(x) = g(x^p)$ para algum polinômio irredutível $g \in K[x]$.*

Demonstração. Pelo Corolário 3.1.21, $f' \equiv 0$. Se $f(x) = \sum_{i=0}^{n} a_i x^i$, então $0 = \sum_{i=1}^{n} i a_i x^{i-1}$ e $i a_i = 0$, $1 \leq i \leq n$. Como $a_i \neq 0$ para algum $i \in \{0, \ldots, n\}$

e $char(K) = p$, temos que $a_i = 0$ sempre que $p \nmid i$. Logo $f(x) = \sum_{j=0}^{n/p} a_{pj}x^{pj} = g(x^p)$, onde $g(x) = \sum_{j=0}^{n/p} a_{pj}x^j$.

Para ver que g é irredutível, observe que se $g = hk$, então $f(x) = h(x^p)k(x^p)$, absurdo, pois f é irredutível. □

3.2 Álgebras de Grupos Abelianos

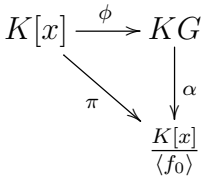
Nesta seção, daremos uma descrição completa de anéis de grupo de um grupo abeliano finito G sobre um corpo K tal que $char(K) \nmid |G|$. Essa descrição foi dada por S. Perlis e G. Walker em 1950 (veja [6]).

Iniciaremos com o caso onde G é cíclico. Assim, assumiremos que $G = \langle a : a^n = 1\rangle$ e que K é um corpo tal que $char(K) \nmid |G|$. Logo, pelo Teorema de Maschke, KG é semissimples. Considere a aplicação $\phi : K[x] \longrightarrow KG$ dada por $\phi(f) = f(a)$.

A aplicação ϕ é um epimorfismo de anéis. De fato, dados f, $g \in K[x]$, temos: $\phi(f+g) = (f+g)(a) = f(a)+g(a) = \phi(f)+\phi(g)$ e $\phi(fg) = (fg)(a) = f(a)g(a) = \phi(f)\phi(g)$. Dado $\beta \in KG$, temos que $\beta = \sum_{j=0}^{n-1} \beta_j a^j$ onde $\beta_j \in K$ e $a^j \in G$ para todo $0 \leq j \leq n-1$. Assim, existe $f(x) = \sum_{j=0}^{n-1} \beta_j x^j \in K[x]$, tal que $\phi(f) = f(a)$. Portanto ϕ é sobrejetora.

Consequentemente, pelo Teorema 1.1.22, $KG \simeq \frac{K[x]}{Ker(\phi)}$, onde $Ker(\phi) = \{f \in K[x] : f(a) = 0\}$. Como $K[x]$ é um domínio de ideais principais, $Ker(\phi)$ é gerado por um polinômio mônico $f_0 \in Ker(\phi)$, de menor grau, tal que $f_0(a) = 0$.

Sob esse isomorfismo, o elemento a é levado para a classe $x + \langle f_0\rangle \in \frac{K[x]}{\langle f_0\rangle}$. Vejamos abaixo:



Temos que $\alpha \circ \phi = \pi$. Logo $(\alpha \circ \phi)(f) = \pi(f) \Rightarrow \alpha(\phi(f)) = f + \langle f_0 \rangle \Rightarrow \alpha(f(a)) = f + \langle f_0 \rangle$. Se $f(x) = x$ então $\alpha(f(a)) = x + \langle f_0 \rangle \Rightarrow \alpha(a) = x + \langle f_0 \rangle$.

Como $a^n = 1$, segue que $x^n - 1 \in Ker(\phi)$. Note que, se $f(x) = \sum_{i=0}^{r} k_i x^i$ é um polinômio não nulo de grau $0 < r < n$, então $f(a) = \sum_{i=0}^{r} k_i a^i \neq 0$. De fato, se $f(a) = 0$, como os elementos $\{1, a, a^2, \ldots, a^r\}$ são linearmente independente sobre K, segue que $k_i = 0$, para todo $0 \leq i \leq r$. Logo $f(x)$ é o polinômio identicamente nulo, absurdo.

Assim, todo polinômio de grau menor que n em $K[x]$, se tem a como raiz, é identicamente nulo. Portanto $x^n - 1$ é o polinômio de menor grau em $Ker(\phi)$. Assim, $Ker(\phi) = \langle x^n - 1 \rangle$ e $KG \simeq \frac{K[x]}{\langle x^n - 1 \rangle}$.

Seja $x^n - 1 = f_1 f_2 \ldots f_t$ uma decomposição de $x^n - 1$ como um produto de polinômios irredutíveis em $K[x]$. Como $char(K) \nmid n$, a derivada de $x^n - 1$ não é o polinômio nulo. Logo, pelo Corolário 3.1.21, $x^n - 1$ não possui raízes múltiplas em nenhuma extensão de K e, consequentemente, f_1,f_2,...,f_t não possui raízes múltiplas em nenhuma extensão de K. Portanto o polinômio é separável, $f_i \neq f_j$ se $i \neq j$, e $mdc(f_i, f_j) = 1$ se $i \neq j$. Temos que $\frac{K[x]}{\langle x^n - 1 \rangle} = \frac{K[x]}{\langle f_1 f_2 \cdots f_t \rangle}$.

Usando o Teorema Chinês dos Restos, obtemos

$$\frac{K[x]}{\langle f_1 f_2 \cdots f_t \rangle} \simeq \frac{K[x]}{\langle f_1 \rangle} \oplus \frac{K[x]}{\langle f_2 \rangle} \oplus \cdots \oplus \frac{K[x]}{\langle f_t \rangle}.$$

Daí, $KG \simeq \frac{K[x]}{\langle f_1 \rangle} \oplus \frac{K[x]}{\langle f_2 \rangle} \oplus \cdots \oplus \frac{K[x]}{\langle f_t \rangle)}$ e, sob esse isomorfismo, a é levado para o elemento $(x + \langle f_1 \rangle, x + \langle f_2 \rangle, \ldots, x + \langle f_t \rangle)$.

Seja ζ_i uma raiz de f_i, $1 \leq i \leq t$, em alguma extensão de K. Então, o Teorema 3.1.12 nos garante que $\frac{K[x]}{\langle f_i \rangle} \simeq K(\zeta_i)$. Consequentemente $KG \simeq K(\zeta_1) \oplus K(\zeta_2) \oplus \cdots \oplus K(\zeta_t)$.

Todas as raízes ζ_i, $1 \leq i \leq t$, são raízes de $x^n - 1$. Logo KG é isomorfo a soma direta de extensões ciclotômicas de K. Sob esse último isomorfismo, o elemento a é levado para o elemento $(\zeta_1, \zeta_2, \ldots, \zeta_t)$.

Vejamos alguns exemplos.

Exemplo 3.2.1. *Sejam $G = C_7$ e $K = \mathbb{Q}$. Nesse caso, a decomposição em polinômios irredutíveis de $x^7 - 1$ em $\mathbb{Q}[x]$ é $x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$. Consequentemente, temos que $\mathbb{Q}G \simeq \mathbb{Q} \oplus \mathbb{Q}(\zeta)$, onde ζ denota uma raiz primitiva da unidade de ordem sete.*

Exemplo 3.2.2. *Sejam $G = C_4$ e $K = \mathbb{Z}_5$. A decomposição em polinômios irredutíveis de $x^4 - 1$ em $\mathbb{Z}_5[x]$ é $x^4 - 1 = (x-1)(x+1)(x-2)(x+2) = (x+1)(x+2)(x+3)(x+4)$. Consequentemente, temos que $\mathbb{Z}_5 C_4 \simeq \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$.*

Exemplo 3.2.3. *A decomposição de $x^6 - 1$ como um produto de polinômios irredutíveis em $\mathbb{Q}[x]$ é $x^6 - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$. Assim $\mathbb{Q}G \simeq \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}\left(\frac{-1+i\sqrt{3}}{2}\right) \oplus \mathbb{Q}\left(\frac{1+i\sqrt{3}}{2}\right) = \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}(\zeta_3) \oplus \mathbb{Q}(\zeta_6)$, onde ζ_3 e ζ_6 são raízes dos polinômios $\Phi_3(x) = x^2 + x + 1$ e $\Phi_6(x) = x^2 - x + 1$ respectivamente.*

Lembremos que, para um inteiro positivo d, o polinômio ciclotômico de ordem d, denotado por Φ_d, é o polinômio $\Phi_d(x) = \prod_j (x - \zeta_j)$, onde ζ_j são as raízes d-ésimas primitivas da unidade. Também sabemos que $x^n - 1 = \prod_{d|n} \Phi_d(x)$, o produto de todos os polinômios ciclotômicos Φ_d em $K[x]$, onde d é um divisor de n.

Nem sempre um polinômio ciclotômico é irredutível sobre K, como por exemplo, se considerarmos $K = \mathbb{C}$, como $\mathbb{C}$ é algebricamente fechado, todo polinômio poderá ser escrito como produto de polinômios de grau 1. Assim, para cada d, considere $\Phi_d = \prod_{i=1}^{a_d} f_{d_i}$ a decomposição de Φ_d como um produto de polinômios irredutíveis em K. Logo, KG pode ser descrito da forma:

$KG \simeq \oplus_{d|n} \frac{K[x]}{\langle \Phi_d(x) \rangle} \simeq \oplus_{d|n} \frac{K[x]}{\langle f_{d_1} f_{d_2} \cdots f_{d_{a_d}} \rangle} \simeq \oplus_{d|n} \oplus_{i=1}^{a_d} \frac{K[x]}{\langle f_{d_i} \rangle} \simeq \oplus_{d|n} \oplus_{i=1}^{a_d} K(\zeta_{d_i})$, onde ζ_{d_i} denota as raízes de f_{d_i}, $1 \leq i \leq a_d$.

Para um d fixo, ζ_{d_i}, $1 \leq i \leq a_d$, são raízes da unidade de ordem d. Como as raízes da unidade formam um grupo multiplicativo $\{1, \zeta_d, \zeta_d^2, \ldots, \zeta_d^{d-1}\}$, temos que $\zeta_{d_i} \in \{1, \zeta_d, \zeta_d^2, \ldots, \zeta_d^{d-1}\}$ para todo $1 \leq i \leq a_d$. Assim, cada ζ_{d_i} é igual a ζ_d^m, para $0 \leq m \leq d-1$, e $K(\zeta_{d_i})$ é o menor corpo que contém K, ζ_{d_i} e todas as potências de ζ_{d_i}. Como para cada i, ζ_{d_i} é uma potência de ζ_d, temos que $K(\zeta_{d_1}) = K(\zeta_{d_2}) = \cdots = K(\zeta_{d_{a_d}})$.

Por isso, todos os corpos da forma $K(\zeta_{d_i})$, $1 \leq i \leq a_d$, são iguais uns aos outros. Além disso, eles também são iguais a $K(\zeta_d)$, pelo mesmo argumento.

Portanto, podemos escrever $KG \simeq \oplus_{d|n} a_d K(\zeta_d)$ onde ζ_d é uma raiz primitiva da unidade de ordem d e $a_d K(\zeta_d)$ denota a soma direta de a_d corpos $K(\zeta_d)$.

Como $deg(f_{d_i}) = [K(\zeta_d) : K]$, os polinômios f_{d_i}, $1 \leq i \leq a_d$, têm o mesmo grau. Observe que $deg(f_{d_1}) + deg(f_{d_2}) + \cdots + deg(f_{d_{a_d}}) = a_d[K(\zeta_d) : K]$ e $deg(f_{d_1}) + deg(f_{d_2}) + \cdots + deg(f_{d_{a_d}}) = deg(\Phi_d) = \varphi(d)$. Assim, $\varphi(d) = a_d[K(\zeta_d) : K]$.

Uma vez que G é um grupo cíclico de ordem n, para cada divisor d de n, o número de elementos de ordem d em G, denotado por n_d, é precisamente $\varphi(d)$. Consequentemente, temos que $a_d = \frac{n_d}{[K(\zeta_d):K]}$.

Exemplo 3.2.4. *Seja $G = C_n$ o grupo cíclico de ordem n e tome $K = \mathbb{Q}$. O polinômio $x^n - 1$ se decompõe em $\mathbb{Q}[x]$ como um produto de polinômios*

ciclotômicos $x^n - 1 = \prod_{d|n} \Phi_d(x)$*, e estes são irredutíveis. Consequentemente,* $\mathbb{Q}G \simeq \oplus_{d|n}\mathbb{Q}(\zeta_d)$.

Encerramos a seção mostrando que a descrição obtida acima pode ser estendida para anéis de grupo sobre grupos abelianos finitos arbitrários. Para dar esta descrição, enunciaremos o seguinte teorema.

Teorema 3.2.5 (Teorema de Estrutura de Grupos Abelianos Finitos)**.** *Todo grupo abeliano finito pode ser escrito como produto direto de grupos cíclicos cuja ordem é uma potência de um primo.*

Com isso, estamos em condições de demonstrar o teorema principal desta monografia.

Teorema 3.2.6 (Perlis-Walker)**.** *Seja* G *um grupo abeliano finito de ordem* n *e seja* K *um corpo tal que* $char(K) \nmid n$*. Então* $KG \simeq \oplus_{d|n} a_d K(\zeta_d)$ *onde* ζ_d *denota uma raiz primitiva da unidade de ordem* d *e* $a_d = \frac{n_d}{[K(\zeta_d):K]}$*. Nessa fórmula,* n_d *denota o número de elementos de ordem* d *em* G*.*

Demonstração. Procedemos por indução na ordem de G. Se $G = \{1\}$, segue o resultado. Suponhamos que o resultado seja válido para todos os grupos abelianos de ordem menor que n. Se G é cíclico, já mostramos que o teorema é válido. Caso contrário, utilizamos o Teorema 3.2.5 para escrever $G = G_1 \times H$, onde H é cíclico, $|G_1| = n_1$, $|H| = n_2$ com n_1, n_2 menores que n.

Por hipótese de indução, escrevemos $KG_1 \simeq \oplus_{d_1|n_1} a_{d_1} K(\zeta_{d_1})$ onde $a_{d_1} = \frac{n_{d_1}}{[K(\zeta_{d_1}):K]}$, n_{d_1} denota o número de elementos de ordem d_1 em G_1 e ζ_{d_1} denota uma raiz primitiva da unidade de ordem d_1. Como H é cíclico, temos $KH \simeq \oplus_{d_2|n_2} a_{d_2} K(\zeta_{d_2})$ onde $a_{d_2} = \frac{n_{d_2}}{[K(\zeta_{d_2}):K]}$, n_{d_2} denota o número de elementos de ordem d_2 em H e ζ_{d_2} é uma raiz primitiva da unidade de ordem d_2. Usando o Lema 1.2.4, a Proposição 1.2.8 e a Proposição 1.3.5, temos que

$$\begin{aligned}
KG &\simeq K(G_1 \times H) \\
&\simeq KG_1 \otimes_K KH \\
&\simeq (\oplus_{d_1|n_1} a_{d_1} K(\zeta_{d_1})) \otimes_K KH \\
&\simeq \oplus_{d_1|n_1} a_{d_1} (K(\zeta_{d_1}) \otimes_K KH)) \\
&\simeq \oplus_{d_1|n_1} a_{d_1} ([K(\zeta_{d_1}) : K]K \otimes_K KH) \\
&\simeq \oplus_{d_1|n_1} a_{d_1} [K(\zeta_{d_1}) : K](K \otimes_K KH) \\
&\simeq \oplus_{d_1|n_1} a_{d_1} [K(\zeta_{d_1}) : K]KH \\
&\simeq \oplus_{d_1|n_1} a_{d_1} [K(\zeta_{d_1}) : K] \oplus_{d_2|n_2} a_{d_2} K(\zeta_{d_2}) \\
&= \oplus_{d_1|n_1} \oplus_{d_2|n_2} a_{d_1} a_{d_2} [K(\zeta_{d_1}) : K] K(\zeta_{d_2}) \\
&\simeq \oplus_{d_1|n_1} \oplus_{d_2|n_2} a_{d_1} a_{d_2} K(\zeta_{d_1}, \zeta_{d_2}).
\end{aligned}$$

Assim, $KG \simeq \oplus_{d_1|n_1} \oplus_{d_2|n_2} a_{d_1} a_{d_2} K(\zeta_{d_1}, \zeta_{d_2})$.

Se considerarmos $d = mmc(d_1, d_2)$, provemos que d divide a ordem do grupo G.

Seja d_1 um divisor da ordem de G_1. Como $G_1 \leq G$, $n_1|n$. Como $d_1|n_1$, por transitividade, $d_1|n$. Analogamente $d_2|n$, onde d_2 é um divisor da ordem do subgrupo H de G.

Como $d_1|n$ e $d_2|n$, temos que $d|n$. Além disso, pelo Teorema 3.1.14, temos que $K(\zeta_{d_1}, \zeta_{d_2}) = K(\zeta_d)$. Assim, $KG \simeq \oplus_{d|n} a_d K(\zeta_d)$ com $a_d = \sum a_{d_1} a_{d_2}$, onde a soma é tomada sobre todos os pares d_1, d_2 tais que $mmc(d_1, d_2) = d$.

Como

$$[K(\zeta_d) : K] = [K(\zeta_{d_1}, \zeta_{d_2}) : K(\zeta_{d_1})][K(\zeta_{d_1}) : K],$$

temos

$$a_d[K(\zeta_d) : K] = \sum_{d_1,d_2} a_{d_1} a_{d_2} [K(\zeta_{d_1}, \zeta_{d_2}) : K(\zeta_{d_1})][K(\zeta_{d_1}) : K] =$$

$$\sum_{d_1,d_2} \frac{n_{d_1}}{[K(\zeta_{d_1}) : K]} \frac{n_{d_2}}{[K(\zeta_{d_2}) : K]} [K(\zeta_{d_1}, \zeta_{d_2}) : K(\zeta_{d_1})][K(\zeta_{d_1}) : K] =$$

$$\sum_{d_1,d_2} n_{d_1} n_{d_2}.$$

Finalmente, note que, como $G = G_1 \times H$, cada elemento $g \in G$ pode ser escrito da forma $g = g_1 h$, com $g_1 \in G$, $h \in H$. Também, podemos ver que $o(g) = mmc(o(g_1), o(h))$. Consequentemente, $\sum_{d_1,d_2} n_{d_1} n_{d_2} = n_d$, o número de elementos de ordem d em G. Assim, temos que $a_d = \frac{n_d}{[K(\zeta_d):K]}$, e o teorema está demonstrado. □

Observemos que, em um grupo abeliano finito, o número de elementos de ordem d é múltiplo de $\varphi(d)$, onde φ é a função de Euler [3, pg. 85]. Logo, o número $a_d = \frac{n_d}{[K(\zeta_d):K]}$ é inteiro.

Exemplo 3.2.7. *Sejam $G = C_2 \times C_2$ e $K = \mathbb{Z}_5$. Pelo teorema de Perlis-Walker, temos que $\mathbb{Z}_5(C_2 \times C_2) \simeq \oplus_{d|4} a_d \mathbb{Z}_5(\zeta_d) \simeq a_1\mathbb{Z}_5(\zeta_1) \oplus a_2\mathbb{Z}_5(\zeta_2) \oplus a_4\mathbb{Z}_5(\zeta_4)$. Como $C_2 \times C_2$ não admite elementos de ordem 4, temos que $\mathbb{Z}_5(C_2 \times C_2) \simeq a_1\mathbb{Z}_5(\zeta_1) \oplus a_2\mathbb{Z}_5(\zeta_2)$. Consequentemente $\mathbb{Z}_5(C_2 \times C_2) \simeq \mathbb{Z}_5 \oplus 3\mathbb{Z}_5 \simeq \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$.*

Se $K = \mathbb{Q}$ no exemplo 3.2.7, temos que $\mathbb{Q}(C_2 \times C_2) \simeq \mathbb{Q} \oplus 3\mathbb{Q} = \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}$.

Corolário 3.2.8. *Seja G um grupo abeliano finito de ordem n. Então*

$$\mathbb{Q}G \simeq \oplus_{d|n} a_d \mathbb{Q}(\zeta_d)$$

onde ζ_d denota uma raiz primitiva da unidade de ordem d e a_d é o número de subgrupos cíclicos de ordem d em G.

Demonstração. Mostramos acima que $a_d = \frac{n_d}{[\mathbb{Q}(\zeta_d):\mathbb{Q}]}$, onde n_d é o número de elementos de ordem d em G. Agora $[\mathbb{Q}(\zeta_d) : \mathbb{Q}] = \varphi(d)$, onde φ denota a função φ de Euler. Note que o número de geradores do grupo cíclico de ordem d é precisamente $\varphi(d)$. Assim, $\frac{n_d}{\varphi(d)}$ é o número de subgrupos de ordem d em G. □

Exemplo 3.2.9. *Sejam $G = C_4$ o grupo cíclico de ordem 4 e $K = \mathbb{Q}$. Então, $\mathbb{Q}C_4 \simeq \oplus_{d|4} a_d\mathbb{Q}(\zeta_d) = a_1\mathbb{Q}(\zeta_1)\oplus a_2\mathbb{Q}(\zeta_2)\oplus a_4\mathbb{Q}(\zeta_4) = \mathbb{Q}\oplus\mathbb{Q}\oplus\mathbb{Q}(i)$. Portanto, $\mathbb{Q}C_4 \simeq \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}(i)$.*

Corolário 3.2.10. *Seja G um grupo abeliano de ordem n e K um corpo tal que $char(K) \nmid n$. Se K contém uma raiz primitiva da unidade de ordem n, então $KG \simeq \underbrace{K \oplus K \oplus \cdots \oplus K}_{n-vezes}$.*

Demonstração. Se K contém uma raiz primitiva da unidade de ordem n, então $K(\zeta) = K$, para todo $d|n$ e o corolário segue diretamente do teorema. □

Se G e H são grupos isomorfos, então as álgebras de grupos KG e KH sobre o corpo K também são isomorfas. Mas a recíproca nem sempre é verdadeira.

Como vimos nos Exemplos 3.2.2 e 3.2.7,

$$\mathbb{Z}_5(C_2 \times C_2) \simeq \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \simeq \mathbb{Z}_5C_4$$

mas $C_2 \times C_2$ não é isomorfo a C_4, pois o grupo $C_2 \times C_2$ não tem elementos de ordem 4.

Este é o primeiro contato com o chamado problema do isomorfismo, que podemos enunciar como segue: sob quais condições um isomorfismo de anéis $RG \simeq RH$ implica $G \simeq H$? Esta é uma motivação para trabalhos futuros.

Bibliografia

[1] M. F. Atiyah, I. G. Macdonald, *Introduction to Commutative Algebra*. Wesley Publishing Company, 128p.

[2] F. U. Coelho, M. L. Lourenço, *Um Curso de Álgebra Linear*. Edusp, (2013), 269p.

[3] J. A. Gallian, *Contemporary Abstracty Algebra*. Cegange Learning, (2012). 664p.

[4] T. W. Hungerford, *Algebra*. Springer, (2012), 504p.

[5] C. P. Milies, S. K. Sehgal. *An Introduction to Group Rings* . Dordrecht, Boston, London: Kluwer Academic Publishers, (2002), 371p.

[6] S. Perlis, G. L. Walker, *Abelian group algebras of finite order*. Trans. Amer. Math. Soc. 68 (1950), 420-426.