Raylso Brambila Costa

Código de grupo cíclico

Alegre - ES

Agosto de 2022

Raylso Brambila Costa

Código de grupo cíclico

Trabalho de conclusão de Curso apresentado ao Departamento de Matemática Pura e Aplicada da Universidade Federal do Espírito Santo como parte dos requisitos para a obtenção do título de Licenciado Pleno em Matemática.

Universidade Federal do Espírito Santo – UFES

Departamento de Matemática Pura e Aplicada

Orientador: Prof. Dr. Victor do Nascimento Martins

Alegre - ES

Agosto de 2022

Raylso Brambila Costa

Código de grupo cíclico

Trabalho de conclusão de Curso apresentado ao Departamento de Matemática Pura e Aplicada da Universidade Federal do Espírito Santo como parte dos requisitos para a obtenção do título de Licenciado Pleno em Matemática.

Trabalho aprovado. Alegre - ES, 04 de agosto de 2022:

Banca examinadora:

gov.br Documento assinado digitalmente
VICTOR DO NASCIMENTO MARTINS
Data: 17/08/2022 17:52:22-0300
Verifique em https://verificador.iti.br

Prof. Dr. Victor do Nascimento Martins (Orientador)
(DMPA/CCENS - UFES)

gov.br Documento assinado digitalmente
ELEONESIO STREY
Data: 17/08/2022 18:48:06-0300
Verifique em https://verificador.iti.br

Prof. Dr. Eleonesio Strey
(DMPA/CCENS - UFES)

gov.br Documento assinado digitalmente
MATHEUS BERNARDINI DE SOUZA
Data: 17/08/2022 19:14:30-0300
Verifique em https://verificador.iti.br

Prof. Dr. Matheus Bernardini de Souza
(FGA - UnB)

Alegre - ES
Agosto de 2022

Agradecimentos

Eu tenho muito a agradecer..

Primeiro, aos meus pais, Rita e Renato, pelo incentivo e apoio incondicional, principalmente nos momentos em que pensei em desistir, sem vocês eu não estaria aqui. Obrigado!

Aos meus irmãos, Ryan e Rayara, que além de irmãos, são meus melhores amigos, são quem eu sei que posso sempre contar, não importa com o que e nem quando, vocês sempre estiveram lá por mim, e eu jamais me esquecerei disso. Obrigado!

A todos os meus amigos: Eduardo, Ravier, CJ, Bazote, Cachopa, Saulo, Luiz e tantos mais que seria até difícil de citar, cada um de vocês, à sua maneira, me deram forças pra seguir, deixaram a universidade mais leve, me fizeram sorrir, me deram sermão quando eu precisei ouvir, e com certeza terão sempre a minha gratidão. Obrigado!

A esses 4 a seguir deixo um parágrafo especial para cada:

Vitor Salgado: Você é meu irmão, você foi e é meu parceiro desde que chegamos aqui, sem você me zoando e me dando café não sei se eu conseguiria concluir esse curso, estaremos sempre juntos, não importa quanto tempo passe.

Pablo Wenceslau: Nem sempre estivemos bem, mas sua amizade se mostrou tão forte que no fim, não posso deixar de te citar aqui. Obrigado pelos sermões, obrigado pelos conselhos, obrigado por me dar força no momento em que mais precisei, você é brilhante e vai longe em tudo que se dispor a fazer. Obrigado!

Eduarda Dutra: O que falar de você? Minha melhor amiga, parceira, companheira. De rolê, de ufes, da vida. Onde quer que eu vá, você estará comigo, se não pessoalmente, com certeza em meu coração, você é genial, e ninguém pode te parar. Você não tem limites, seu coração é puro e sua vontade de prosperar pode e vai superar qualquer barreira que você encontre, não há nada nesse mundo que você não seja capaz de fazer, e é por isso que te admiro tanto e estarei lá para ver e comemorar com você cada passo que der em direção aos seus objetivos. Obrigado!

Robert Vinícius: Infelizmente você não está aqui para dizer que esses agradecimentos estão muito dramáticos, mas lá vai: Você foi a primeira pessoa que estendeu a mão para mim quando eu cheguei em Alegre, rapidamente se tornou meu irmão e eu queria ter dito isso mais vezes para você, você é meu herói, e eu sempre levarei você comigo. Obrigado!

Aos professores da Universidade Federal do Espírito Santo, em particular, ao Prof. Dr. Eleonesio Strey, pelos ensinamentos e orientação no meu projeto de iniciação científica.

À instituição Universidade Federal do Espírito Santo por todo o suporte e estrutura que me foram fornecidos nesses 5 anos em que estive por aqui.

Aos prof. Dr. Matheus Bernardini de Souza e prof. Dr. Eleonesio, meus sinceros agradecimentos por aceitarem avaliar meu trabalho e por todas as correções e contribuições.

E claro, ao meu orientador e amigo, Prof. Dr. Victor Martins, por toda a sua ajuda na minha formação, eu sei que me orientar não foi uma tarefa fácil, e como resultado disso, tivemos algumas dificuldades e obstáculos para a produção desse TCC. No entanto, graças à sua determinação e imensa paciência comigo, fomos capazes de superar essas barreiras e concluir o trabalho. Talvez você não saiba disso, mas você foi um dos principais responsáveis para que eu chegasse até aqui, você é inspiração para mim e para muitos outros. Obrigado!

Resumo

Nesse trabalho de conclusão de curso, apresentamos os códigos corretores de erros sob o ponto de vista algébrico. Os benefícios ao mesclar códigos e estruturas algébricas são essenciais para todos: melhores e mais sofisticados algoritmos de codificação e decodificação de erros. Neste sentido, a pergunta que norteou a nossa investigação foi: a que estrutura algébrica corresponde um código cíclico quando definido sobre uma álgebra de grupo? Partindo dessa pergunta, o objetivo do trabalho envolve enxergar códigos sobre diferentes estruturas algébricas, para assim, conseguir realizá-los sobre álgebras de grupo.

Palavras-chave: Códigos corretores de erros; Códigos cíclicos; Álgebra de grupo; Estruturas algébricas.

Sumário

Introdução **7**

1 PRELIMINARES ALGÉBRICOS **12**
1.1 Grupos **12**
1.2 Anéis e corpos **13**
1.2.1 O anel de polinômios 18
1.2.2 Corpos finitos 21

2 CÓDIGOS LINEARES **22**
2.1 Equivalência de códigos **23**
2.2 Matriz Geradora de um código **25**
2.3 Códigos Duais **27**
2.4 Códigos cíclicos **28**
2.4.1 Matrizes geradoras e teste de paridade de um código cíclico 30
2.4.2 Codificação em Códigos Cíclicos 33

3 ÁLGEBRAS DE GRUPO **36**
3.1 Módulos **36**
3.1.1 Módulos semissimples 40
3.2 Ánéis de grupo **42**
3.2.1 Ideais de aumento 45
3.2.2 Semissimplicidade 47
3.2.3 Álgebras de grupos abelianos 51

4 CÓDIGOS CÍCLICOS SOBRE ÁLGEBRAS DE GRUPO **54**
4.1 Códigos de grupo **54**
4.2 Códigos sobre álgebras de grupo cíclico **55**
4.3 Matrizes geradora e teste de paridade **57**
4.4 Zeros do Código Cíclico **60**

Considerações Finais **63**

REFERÊNCIAS **64**

Introdução

Os códigos corretores de erros estão em praticamente todo sistema de envio de informações que conhecemos, como assistir um vídeo no Youtube, mandar mensagem pelo Whatsapp ou ao fazer uma ligação por exemplo. Um código corretor de erros nada mais é do que uma maneira organizada de transmitir uma mensagem, isto é, ele nos permite ao receber uma informação, que seja possível detectar e corrigir erros, garantindo segurança ao usuário. Além disso, códigos corretores de erros podem ser usados para esconder informações e também ajudar a lidar com a invasão de hackers.

A teoria surgiu no final dos anos 40, quando o matemático americano C. E. Shanon, do Laboratório Bell, se questionou sobre o porque as máquinas não eram capazes de encontrar a posição de um determinado erro e corrigí-lo, uma vez que elas podiam detectá-lo.

Vejamos um exemplo familiar de um código corretor de erros para que fique mais claro. Vamos considerar um idioma. Seja $\mathcal{A}$ o alfabeto brasileiro. Vamos denotar por $\mathcal{P}$ o conjunto das palavras da língua portuguesa. Uma palavra da língua portuguesa pode ser considerada um elemento de $\mathcal{A}^{46}$, onde 46 é a quantidade de letras da maior palavra de $\mathcal{P}$, a saber, *pneumoultramicroscopicossilicovulcanoconiótico*. Agora, note que $\mathcal{P}$, é um subconjunto próprio de $\mathcal{A}^{46}$, o que faz com que esse código seja detector e corretor de erros. De fato, suponha que ao enviar a mensagem "saudade" ocorresse alguma interferência de modo que a palavra recebida foi, na verdade, "sautade". Como essa palavra não pertence a $\mathcal{P}$, percebe-se imediatamente que houve erro, e corrigí-lo é muito simples, já que a palavra em $\mathcal{P}$ que mais se aproxima de "sautade" é "saudade".

Agora suponha que ao enviar a mensagem "gato" ocorra erro em que a mensagem recebida seja "rato". Diferente do exemplo anterior, a detecção desse erro será muito dificil, já que "rato" também pertence a $\mathcal{P}$. Contudo, suponha que depois de certo esforço foi possível detectar a existência de um erro. Um pensamento natural seria pensar em como corrigí-lo, o que também não seria tarefa fácil, porque existem mais palavras em $\mathcal{P}$ que se parecem com "gato", como por exemplo as palavras "tato", "nato" e "pato". Isso acontece porque um idioma não é um código muito eficiente, pois nele existem palavras muito "próximas" uma das outras.

Quando falamos em códigos, estamos lidando fundamentalmente com ferramentas digitais, então, nesse processo de transmissão de informações, primeiro é preciso converter essas informações em sinal digital, ou melhor, codificá-las, para só então serem transmitidas. Entretanto, assim como no código do idioma, no momento da transmissão a mensagem pode ser adulterada pela interferência de ruídos (ou erros), que se dão por causa do meio

físico utilizado (computadores, celulares, etc), os chamados **canais**. Assim, os canais são melhorados para reduzir a possibilidade de ruído, evitando que eventuais erros possam surgir por causa do mal uso desses equipamentos ou até mesmo aleatoriamente. Para resolver este problema, foram traçadas algumas estratégias, a mais comum é a técnica de repetição, onde a mesma mensagem é transmitida várias vezes e depois todas as recepções são comparadas, pois elas podem ajudar na reconstrução da mensagem original. É claro que não é possível garantir que a mensagem será reconstruída corretamente todas as vezes, essa questão deve ser encarada em termos probabilísticos.

Como essas repetições são realizadas através de equipamentos físicos, elas geram custo, que pode ser entendido como o tempo gasto no processo, custo financeiro ou mesmo na capacidade dos computadores. Na verdade, as repetições só multiplicam esse custo, então é preciso encontrar um balanço entre custo e confiabilidade na transmissão, sabendo que quanto maior for a quantidade de repetições, maior será a confiança de que a mensagem será entregue corretamente, ao mesmo passo que quanto maior for a quantidade de repetições, maior será o custo.

Vejamos um exemplo mais elaborado de um código para ilustrar os princípios da teoria. Suponha um helicóptero de controle remoto, onde suas únicas direções possíveis de vôo são norte, sul, leste, oeste, sudeste, nordeste, sudoeste e noroeste. Tomando $A = \{0, 1\}$, os oito movimentos podem ser codificados em elementos de $\{0, 1\} \times \{0, 1\} \times \{0, 1\}$, como no diagrama abaixo.

$$\begin{array}{ll} \text{Leste} \mapsto 000 & \text{Nordeste} \mapsto 110 \\ \text{Oeste} \mapsto 001 & \text{Sudeste} \mapsto 101 \\ \text{Norte} \mapsto 011 & \text{Noroeste} \mapsto 010 \\ \text{Sul} \mapsto 100 & \text{Sudoeste} \mapsto 111 \end{array}$$

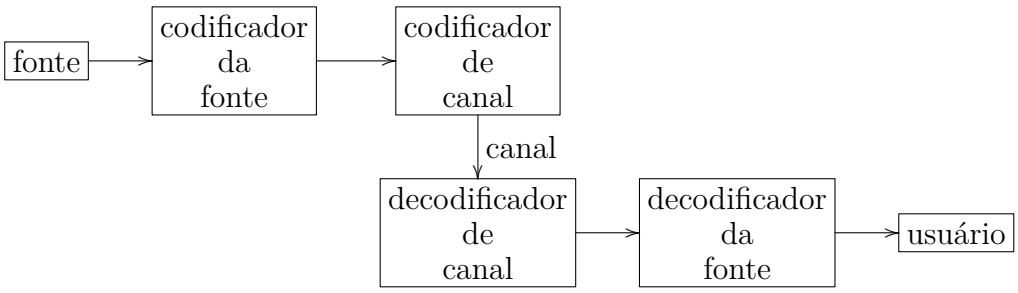
O código numérico à direita é chamado de **código da fonte**. Imaginemos que ao enviar a mensagem 011, aconteça uma interferência fazendo com que a mensagem recebida seja 010, isso faria com que o helicóptero fosse para noroeste ao invés de ir para o norte. Para evitar com que isso aconteça, o que se faz é recodificar as palavras, introduzindo uma série de redundâncias que permitam detectar e corrigir erros. Agora em $\{0, 1\}^6$.

$$\begin{array}{ll} \text{Leste} \mapsto 000000 & \text{Nordeste} \mapsto 110010 \\ \text{Oeste} \mapsto 001011 & \text{Sudeste} \mapsto 101110 \\ \text{Norte} \mapsto 011100 & \text{Noroeste} \mapsto 010111 \\ \text{Sul} \mapsto 100101 & \text{Sudoeste} \mapsto 111001 \end{array}$$

O novo código introduzido é chamado de **código de canal**. Suponhamos que ao se transmitir a mensagem 110010, tenha ocorrido um erro de modo que a palavra recebida

foi 111010, é fácil notar que essa última não pertence ao código, portanto, a detecção do erro é possível. Comparando essa mensagem com as do código, vemos que a que "mais se aproxima" de 111010 é 110010, que é precisamente a mensagem inicialmente transmitida.

A teoria de códigos tem como objetivo transformar o código da fonte em código de canal, em detectar e corrigir erros e em decodificar o código de canal em código da fonte. Estes são os chamados processos de **codificação** e **decodificação**, e é isso que está exemplificado no diagrama a seguir:



O estudo da teoria de códigos tem como um de seus principais pilares encontrar algoritmos de codificação e decodificação cada vez melhores, por isso a ideia de mesclar códigos com estruturas algébricas é bastante promissora, uma vez que ao realizarmos códigos sobre estruturas algébricas ganhamos todas as ferramentas dessas estruturas na busca por processos de codificação e decodificação mais eficientes.

Neste trabalho, discorremos sobre os chamados códigos lineares, que são códigos sobre espaços vetoriais. Nesse tipo de código, o nosso alfabeto é um corpo finito $\mathbb{K}$, as palavras do código são elementos de $\mathbb{K}^n$ e um código C é um subespaço vetorial de $\mathbb{K}^n$. Esses códigos são importantes porque eles possuem baixo custo do ponto de vista do processamento de codificação e decodificação de mensagens, o que é de suma importância na teoria. Vale ressaltar que o processo de transmissão de informações é realizado por computadores, então a existência de códigos de processamento é essencial, e é por isso que os códigos desse tipo são os mais utilizados na prática. Mas além disso, há também uma outra razão para explorar esse tipo de código, pois percebeu-se ao longo do desenvolvimento da teoria, que é possível associar alguns códigos lineares, os chamados códigos cíclicos, a ideais de um anel, nos fornecendo melhores algoritmos para detecção e correção de erros e ainda, que também é possível associá-los a ideais em anéis de grupo, uma estrutura que une as estruturas de anel e grupo. Além disso, os códigos cíclicos tem a vantagem de permitirem que seus parâmetros (dimensão do código, dimensão do espaço, e distância mínima) sejam rapidamente determinados.

Os parâmetros de um código são parte importante no processo de codificação e decodificação. Um desses parâmetros trata de uma maneira de medir o quão próximas estão as palavras de um código. Dadas $\mathbf{u}, \mathbf{v} \in \mathbb{K}^n$ duas palavras, a **distância de Hamming**

entre $\mathbf{u} = (u_1, \ldots, u_n)$ e $\mathbf{v} = (v_1, \ldots, v_n)$ é definida como

$$d(\mathbf{u}, \mathbf{v}) = |\{i : u_i \neq v_i, \ \ 1 \leq i \leq n\}|.$$

Por exemplo, em $\{0,1\}^3$ temos que se $\mathbf{u} = (1,0,1)$ e $\mathbf{v} = (1,1,0)$, então $d(\mathbf{u}, \mathbf{v}) = 2$.

Note que o princípio da boa ordenação garante que esse conjunto tenha um elemento mínimo. Então, se $C \subset \mathbb{K}^n$ é um código linear, chamaremos de **distância mínima** de C o número

$$d = \min\{d(\mathbf{u}, \mathbf{v}) : \mathbf{u}, \mathbf{v} \in C \text{ e } \mathbf{u} \neq \mathbf{v}\}.$$

Por exemplo, se C é o código do helicóptero, temos $d = 3$. Note que para calcular d é necessário calcular $\binom{n}{2}$ distâncias, onde n é o número de palavras do código, o que pode ser muito trabalhoso. Uma grande importância da distância mínima de um código é no que diz respeito a capacidade de detecção e correção de erros do código, já que se C é um código linear com distância mínima d, então C pode corrigir até $\left[\frac{d-1}{2}\right]$ erros e detectar até $d-1$ erros, onde $[t]$ é a parte inteira de um número real t.

Procuramos apresentar neste texto uma breve introdução à teoria dos códigos, para em especial enfatizar a utilização de diferentes estruturas algébricas a fim de obter melhores algoritmos de codificação e decodificação. Iremos nos dedicar a apresentar mais detalhes sobre os códigos cíclicos, importante subclasse dos códigos lineares. Para atingir nosso objetivo dividimos o trabalho em quatro capítulos.

No Capítulo 1, apresentamos os preliminares algébricos necessários para compreensão do restante do texto. Em especial, trazemos as definições e resultados básicos da teoria de grupos e de anéis e corpos. Optamos por omitir neste capítulo os conceitos básicos de álgebra linear. Apesar de serem essenciais, entendemos que a inserção de tópicos de álgebra linear no texto tornaria nosso trabalho extenso e talvez cansativo para o leitor. Para uma revisão dos tópicos de álgebra linear mais importantes para leitura deste trabalho, sugerimos uma consulta aos capítulos 3, 5 e 6 de (HEFEZ; FERNANDEZ, 2016).

No Capítulo 2, trazemos a teoria básica de códigos. Já direcionamos este capítulo para os códigos lineares que são nosso objeto de estudo. Utilizamos esse capítulo para dar as primeiras definições matemáticas dentro da teoria e já explorar as primeiras estruturas algébricas que aparecerão: espaços vetoriais e anéis. A teoria de anéis surge na última seção do Capítulo 2, ao falarmos dos códigos cíclicos. E as discussões que ali aparecerão, serão revisitas no capítulo final do trabalho.

No Capítulo 3, iremos introduzir uma outra estrutura algébrica. Uma estrutura híbrida entre a teoria de grupos e a teoria de anéis chamada anéis de grupo. Nosso principal objetivo nesse trabalho é realizar códigos cíclicos sobre essa nova estrutura. Portanto, mesmo que omitindo alguns resultados e demonstrações importantes sobre anéis de grupo, procuramos fazer um capítulo objetivo, mas ao mesmo tempo completo o suficiente, para total compreensão da parte final do trabalho.

Por fim, no Capítulo 4, basicamente o que fazemos é juntar toda a informação obtida no Capítulo 2 sobre os códigos cíclicos, utilizando as estruturas de espaço vetorial e anel, com a teoria de anéis de grupo desenvolvida no Capítulo 3, para enxergar os mesmos códigos sobre essa nova estrutura.

Entre outras coisas, nossa proposta procura evidenciar a importância do estudo de códigos sobre estruturas algébricas observando as vantagens dessa utilização e mostrando como a matemática pura está intrinsicamente ligada a assuntos cotidianos. Além disso, também acreditamos que este texto possa servir de base para quem deseja começar os estudos em teoria de códigos sobre o ponto de vista algébrico, já que tentamos apresentar os conceitos de maneira bem clara, indicando referências que complementam nossa apresentação dos conceitos envolvidos. O único pré-requisito necessário para um melhor aproveitamento do trabalho é um curso introdutório de álgebra linear.

1 Preliminares algébricos

Neste capítulo traremos alguns resultados importantes sobre as estruturas algébricas básicas que serão utilizadas no decorrer do trabalho. Para mais detalhes sobre a teoria básica de grupos e anéis, sugerimos (GONÇALVES, 2017) e para um estudo da teoria de anéis mais direcionado ao que se é utilizado na teoria de códigos cíclicos, indicamos (HEFEZ; VILLELA, 2008). No decorrer do trabalho indicaremos por $\mathbb{N} = \{1, 2, 3, \dots\}$ o conjunto dos números naturais e $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

1.1 Grupos

Seja G um conjunto não vazio munido de uma operação que denotaremos por $*$:

$$\begin{aligned} * : G \times G &\to G \\ (a, b) &\mapsto a * b \end{aligned}$$

Chamaremos o par $(G, *)$ de **grupo** se para quaisquer $a, b, c \in G$ forem satisfeitas as seguintes propriedades:

(G1) $(a * b) * c = a * (b * c)$;

(G2) Existe um elemento $e \in G$, chamado **identidade** de G, tal que $a * e = e * a = a$;

(G3) Existe um elemento chamado **simétrico** ou **inverso** de a e denotado por $a^{-1} \in G$, tal que $a * a^{-1} = e$.

Definição 1.1. Seja $(G, *)$ um grupo. Dizemos que G é um grupo **abeliano** se: (G4) para quaisquer $a, b \in G, a * b = b * a$.

Exemplo 1.1. (a) Dado $n \in \mathbb{N}, n \geq 2$, o conjunto das classes dos inteiros módulo n dado por $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \dots, \overline{n-1}\}$ é um grupo finito com a adição usual contendo n elementos.

(b) Seja

$$S_n = \{f : \{1, 2, \dots, n\} \mapsto \{1, 2, \dots, n\} : f \text{ é bijetiva}\}.$$

O par $(S_n, \circ)$, onde $\circ$ denota a composição de funções, é um grupo, chamado **grupo das permutações** de $\{1, 2, \dots, n\}$. O número de elementos de S_n é $n!$.

A partir de agora, a menos que mencionemos o contrário, G denotará um grupo $(G, *)$ e ao operarmos dois elementos a e b em G poderemos substituir $a * b$ simplesmente pela justaposição dos elementos, ab.

Seja G um grupo e $a \in G$. Se $n \in \mathbb{Z}$, definimos a^n por:

$$a^n = \begin{cases} e & \text{se } n = 0 \\ a^{n-1} * a & \text{se } n > 0 \\ (a^{-n})^{-1}, & \text{se } n < 0 \end{cases}$$

Se $m, n \in \mathbb{Z}$ temos que $a^m * a^n = a^{m+n}$ e $(a^m)^n = a^{mn}$. Definimos

$$\langle a \rangle = \{a^m : m \in \mathbb{Z}\} \subset G.$$

Como $a^0 = e, (a^m)^{-1} = a^{-m}$ e $a^m * a^n = a^{m+n}$, segue que $\langle a \rangle$ é um grupo abeliano. O grupo $\langle a \rangle$ é chamado **grupo cíclico** gerado por $a \in G$. Um grupo G é dito **cíclico** se existe $a \in G$ tal que $G = \langle a \rangle$, neste caso, a é dito um **gerador** de G. É fácil ver que todo grupo cíclico é abeliano.

Exemplo 1.2. (a) $(\mathbb{Z}_p, +)$, com p primo é um grupo cíclico sendo que todos os seus elementos não nulos geram o grupo.

Definição 1.2. Sejam G um grupo e H um subconjunto não vazio de G. Dizemos que H é um **subgrupo** de G se H for ele próprio um grupo com a mesma operação de G.

Exemplo 1.3. (i) Dado $n \in \mathbb{Z}$, o conjunto $H = n\mathbb{Z} = \{nz : z \in \mathbb{Z}\}$ é um subgrupo do grupo aditivo dos inteiros.

(ii) Seja G um grupo e $a \in G$, então $H = \langle a \rangle$ é um subgrupo de G.

(iii) Seja G um grupo e $a \in G$, então $C_G(a) = \{b \in G : ba = ab\}$ é um subgrupo de G chamado **centralizador** de a em G.

(iv) Seja G um grupo. Chamamos de **centro** de G o seguinte conjunto

$$Z(G) = \{a \in G : ab = ba, \forall b \in G\}.$$

O centro $Z(G)$ de G é um subgrupo abeliano de G.

1.2 Anéis e corpos

Seja R um conjunto não vazio munido de duas operações que chamaremos de adição e multiplicação e denotaremos, respectivamente, por $+$ e $\cdot$:

$$+ : R \times R \to R \qquad \text{e} \quad \cdot : R \times R \to R$$
$$(a, b) \mapsto a + b \qquad\qquad (a, b) \mapsto a \cdot b$$

Chamaremos o sistema $(R, +, \cdot)$ de anel se para quaisquer $a, b, c \in R$ forem satisfeitas as seguintes propriedades:

(R1) $(a + b) + c = a + (b + c)$;

(R2) $a + b = b + a$;

(R3) Existe um **elemento neutro** $0 \in R$, chamado de **zero**, tal que $a + 0 = 0 + a = a$;

(R4) Existe $-a \in R$ tal que $a + (-a) = 0$;

(R5) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

(R6) $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(b + c) \cdot a = b \cdot a + c \cdot a$.

Definição 1.3. Seja $(R, +, \cdot)$ um anel.

- R é dito um **anel com unidade** se:

  (R7) existe um elemento $1 \in R$, chamado **unidade**, tal que $0 \neq 1$ e $a \cdot 1 = a = 1 \cdot a$, para todo $a \in R$;

- R é dito um anel comutativo se:

  (R8) para quaisquer $a, b \in R, a \cdot b = b \cdot a$;

- R é dito um **anel sem divisores de zero** se:

  (R9) para quaisquer $a, b \in R$ vale a implicação $a \cdot b = 0 \implies a = 0$ ou $b = 0$;

- R é dito um **domínio de integridade** ou **anel de integridade** se R for um anel comutativo, com unidade e sem divisores de zero;

- R é dito um **corpo** se R for um anel comutativo com unidade e ainda for satisfeita a seguinte propriedade:

  (R10) para todo $a \in R, a \neq 0$, existe $x \in R$ tal que $a \cdot x = 1$. Neste caso, chamamos x de **inverso** de a e o denotamos por a^{-1}.

Exemplo 1.4. (a) Dado $n \in \mathbb{N}$, considere o conjunto $n\mathbb{Z} = \{n \cdot z : z \in \mathbb{Z}\}$.

- $n\mathbb{Z}$ é um anel comutativo para todo $n \geq 1$;

- $n\mathbb{Z}$ é um anel sem divisores de zero para todo $n \geq 1$;
- $n\mathbb{Z}$ não possui unidade para todo $n \geq 2$.

(b) Dado $n \in \mathbb{N}, n \geq 2$, considere o conjunto $\mathbb{Z}_n$.

- $\mathbb{Z}_n$ é anel comutativo com unidade;
- se n é primo, então $\mathbb{Z}_n$ é um corpo.

Sejam $(R, +, \cdot)$ um anel e $B \subset R$. Se $(B, +, \cdot)$ for um anel, dizemos que B é um **subanel** de R, isto é, se B for um subconjunto de R que herda a estrutura de anel de R.

Definição 1.4. Seja R um anel com unidade $1 \in R$. Dizemos que um elemento $e \in R, e \neq 0$ é um idempotente de R se $e^2 = e$.

Dado $e \in R$ um idempotente de R, os conjuntos $R_1 = R \cdot e = \{a \cdot e : a \in R\}$ e $R_2 = R \cdot (1 - e) = \{a - a \cdot e : a \in R\}$ são subanéis de R tais que $R_1 \cap R_2 = \{0\}$ e além disso, para todo $a \in R$, existem únicos elementos $a_1 \in R_1$ e $a_2 \in R_2$ tais que $a = a_1 + a_2$, neste caso, escrevemos $R = R_1 \oplus R_2$ e dizemos que R é **soma direta** dos subanéis R_1 e R_2.

Definição 1.5. Um subanel $I \subset R$ é um **ideal à esquerda** de R se $a \cdot x \in I$, para todo $a \in R$ e para todo $x \in I$ (simbolicamente $R \cdot I \subset I$). Dizemos ainda que I é um **ideal à direita** de R se $x \cdot a \in I$, para todo $a \in R$ e para todo $x \in I$ (simbolicamente $I \cdot R \subset I$). Se I é um ideal à esquerda e à direita simultaneamente, dizemos que I é um **ideal** de R, isto é,

$$R \cdot I \subset I \text{ e } I \cdot R \subset I.$$

Enunciarmos a seguir uma proposição que nos permite verificar quando um subanel I é um ideal(à esquerda) de um anel R. O resultado é análogo para ideais à direita.

Proposição 1.1. *Seja $(R, +, \cdot)$ um anel com unidade. Então $I \subset R$ é um ideal (à esquerda) de R se, e somente se, as seguintes condições são verificadas:*

(i) $x + y \in I$, *para todos* $x, y \in I$.

(ii) $a \cdot x \in I$, *para todo* $x \in I$ *e para todo* $a \in R$.

Se R é um anel, os conjuntos $\{0\}$ e R são ideais de R e são chamados **ideais triviais** de R. Os ideais não triviais de R são chamados **ideais próprios** de R. Um anel é chamado de **anel simples** se seus únicos ideais são os triviais.

Seja R um anel. Um ideal $I \subset R$ é dito **ideal principal à esquerda (à direita)** se existe $\alpha \in R$ tal que $I = R\alpha$ ($I = \alpha R$). Se $I = \alpha R = R\alpha$, I é dito simplesmente **ideal**

principal. Um domínio de integridade no qual todo ideal é principal é chamado **domínio principal** ou **anel principal**.

Por exemplo, $n\mathbb{Z}$ é um domínio principal. De fato, seja I um ideal de $\mathbb{Z}$. Se $I = \{0\}$, então I é gerado por $0 \in \mathbb{Z}$. Suponha que $I \neq \{0\}$. Daí, considere n o menor elemento positivo de I. Seja $a \in I$. Pelo algorítmo da divisão,

$$a = qn + r \implies r = a - qn, \text{ onde } 0 \leq r < nr.$$

Como $r \in I, r < n$ e n é o menor inteiro positivo de I, segue que $r = 0$. Isto é, $a = qn$. Desta forma, todo elemento de I é um múltiplo de n e, portanto, $I = n\mathbb{Z}$.

Definição 1.6. Sejam R um anel e $I \subset R$ um ideal de R. Dizemos que I é um **ideal maximal** em R se $I \neq R$ e os únicos ideais de R contendo I são I e R, isto é, se $J \subset R$ é ideal e $I \subset J$ então $J = I$ ou $J = R$. Por outro lado, I será um **ideal minimal** em R se $I \neq 0$ e os únicos ideais de R contidos em I são os triviais, isto é, se $J \subset R$ é ideal e $J \subset I$ então $J = \{0\}$ ou $J = I$.

Teorema 1.1 (Teorema 3.3, (GONÇALVES, 2017))**.** *Seja* $(\mathbb{K}, +, \cdot)$ *um anel comutativo com unidade* $1 \in \mathbb{K}$*. Então as seguintes condições são equivalentes:*

(i) $\mathbb{K}$ *é um corpo;*

(ii) $\{0\}$ *é um ideal maximal em* $\mathbb{K}$*;*

(iii) os únicos ideais de $\mathbb{K}$ *são os triviais.*

Sejam R um anel qualquer e J um ideal de R. Defina a seguinte relação em R

$$x, y \in R, x \equiv y \pmod{J} \iff x - y \in J.$$

A relação $x \equiv y \pmod{J}$ é lida da seguinte maneira "x é congruente a y módulo J". Verifica-se que a relação definida é uma relação de equivalência em R, isto é, reflexiva, simétrica e transitiva. Se $x \in R$, então

$$\overline{x} = \{y \in R : y \equiv x \pmod{J}\}$$

é a classe de equivalência do elemento $x \in R$ relativamente a relação $\equiv \pmod{J}$. Note que, se $y \in \overline{x}$ então

$$y - x \in J \iff y - x = j, \text{ para algum } j \in J \iff y = x + j, \text{ para algum } j \in J.$$

Por isso, também denotamos a classe de x por $\overline{x} = x + J = \{x + z : z \in J\}$.

O conjunto quociente

$$\frac{R}{J} = \{\overline{x} = x + J : x \in R\}$$

dado por essa relação de equivalência, munido das operações de adição e multiplicação definidas por

$$+ : \frac{R}{J} \times \frac{R}{J} \to \frac{R}{J} \qquad \text{e} \quad \cdot : \frac{R}{J} \times \frac{R}{J} \to \frac{R}{J}$$
$$(\overline{x}, \overline{y}) \mapsto \overline{x} + \overline{y} = \overline{x+y} \qquad (\overline{x}, \overline{y}) \mapsto \overline{x} \cdot \overline{y} = \overline{x \cdot y}$$

é um anel chamado **anel quociente** de R por J. Além disso, se 1 é a unidade de R então $\overline{1}$ é a unidade de $\dfrac{R}{J}$ e se R é comutativo então $\dfrac{R}{J}$ é comutativo.

Teorema 1.2 (Teorema 3.7, (GONÇALVES, 2017))**.** *Sejam R um anel comutativo com unidade $1 \in R$ e J um ideal de R. Então*

$$J \text{ é um ideal maximal em } R \iff \frac{R}{J} \text{ é um corpo.}$$

Observe que esse teorema nos dá uma forma de construir corpos a partir de um anel R comutativo com unidade, basta procurarmos seus ideais maximais.

Exemplo 1.5. O anel quociente dos inteiros módulo n é

$$\mathbb{Z}_n = \frac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Se p é primo, então $p\mathbb{Z}$ é um ideal maximal em $\mathbb{Z}$, logo $\mathbb{Z}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$ é um corpo.

Sejam R e S dois anéis. Uma aplicação $f : R \to S$ é um **homomorfismo** de R em S se satisfaz

(i) $f(x+y) = f(x) + f(y)$, para todos $x, y \in R$;

(ii) $f(x \cdot y) = f(x) \cdot f(y)$, para todos $x, y \in R$.

Se $f : R \to S$ é um homomorfismo bijetor dizemos que f é um **isomorfismo**. Neste caso, dizemos que R e S são isomorfos e denotamos por $R \simeq S$.

Sejam R e S anéis e $f : R \to S$ um homomorfismo entre esses anéis. Chamamos de **núcleo** de f o conjunto definido por

$$\ker(f) = \{a \in R : f(a) = 0\} \subset R.$$

E chamamos de **imagem** de f o conjunto definido por

$$Im(f) = \{f(a) : a \in R\} \subset S.$$

Pode-se mostrar que se $f : R \to S$ é um homomorfismo de anéis, então $Im(f)$ é um subanel de S, $\ker(f)$ é um ideal de R e que f é injetivo se, e somente se, $\ker(f) = \{0\}$.

Teorema 1.3. ***(Teorema do homomorfismo de anéis)*** *Seja $f : R \mapsto S$ um homomorfismo de anéis. Então os anéis $\dfrac{R}{\ker(f)}$ e $Im(f)$ são isomorfos.*

1.2.1 O anel de polinômios

Seja $\mathbb{K}$ um corpo qualquer. Um **polinômio** sobre $\mathbb{K}$ na indeterminada x é uma expressão formal $f(x) = a_0 + a_1x + \cdots + a_mx^m + \cdots$, em que $a_i \in \mathbb{K}$, para todo $i \in \mathbb{N}_0$ e existe $n \in \mathbb{N}_0$ tal que $a_j = 0$, para todo $j \geq n$.

Dois polinômios $f(x) = a_0+a_1x+\cdots+a_mx^m+\cdots$ e $g(x) = b_0+b_1x+\cdots+b_kx^k+\cdots$ são iguais se, e somente se, $a_i = b_i$, para todo $i \in \mathbb{N}_0$.

Se $f(x) = 0 + 0x + \cdots + 0x^m + \cdots$ indicaremos $f(x)$ por 0 e o chamaremos de **polinômio identicamente nulo** sobre $\mathbb{K}$.

Se $a \in \mathbb{K}$ indicaremos por a ao polinômio $f(x) = a_0 + a_1x + \cdots + a_mx^m + \cdots$ onde $a_0 = a$ e $a_i = 0$, para todo $i \geq 1$.

Chamamos o polinômio $f(x) = a, a \in \mathbb{K}$ de **polinômio constante** a.

Se $f(x) = a_0 + a_1x + \cdots + a_mx^m + \cdots$ é tal que $a_n \neq 0$ e $a_j = 0$ para todo $j > n$ dizemos que n é o **grau** do polinômio $f(x)$ e, neste caso indicamos

$$f(x) = a_0 + a_1x + \cdots + a_nx^n,$$

e o grau de $f(x)$ por $gr(f(x)) = n$. Note que não está definido o grau do polinômio identicamente nulo.

Vamos denotar por $\mathbb{K}[x]$ o conjunto de todos os polinômios sobre $\mathbb{K}$, na indeterminada x. Desta forma, o grau pode ser interpretado como uma função gr do conjunto de todos os polinômios não nulos no conjunto $\mathbb{N}_0$. Assim,

$$\begin{aligned} gr : \mathbb{K}[x] \setminus \{0\} &\to \mathbb{N}_0 \\ f(x) &\mapsto gr(f(x)) \end{aligned}$$

Com as operações usuais de soma e multiplicação de polinômios, $\mathbb{K}[x]$ é um domínio de integridade, onde o polinômio 0 é o elemento neutro e o polinômio constante 1 é a unidade.

Teorema 1.4 (Algoritmo da Divisão)**.** *Sejam $f(x), g(x) \in \mathbb{K}[x]$ e $g(x) \neq 0$. Existem únicos $q(x), r(x) \in \mathbb{K}[x]$ tais que*

$$f(x) = q(x) \cdot g(x) + r(x),$$

onde $r(x) = 0$ ou $gr(r(x)) < gr(g(x))$.

Se $f(x) = a_0 + a_1x + \cdots + a_nx^n$ é um polinômio não nulo em $\mathbb{K}[x]$ e $\alpha \in \mathbb{K}$ é tal que $f(\alpha) = 0 \in \mathbb{K}$, diremos que α é uma **raíz** de $f(x)$ em $\mathbb{K}$. A seguir enunciaremos uma proposição que limita a quantidade de raízes em um corpo $\mathbb{K}$.

Proposição 1.2. *Seja $\mathbb{K}$ um corpo e seja $f(x)$ um polinômio não nulo em $\mathbb{K}[x]$ de grau n, então $f(x)$ tem no máximo n raízes em $\mathbb{K}$.*

Observe, por exemplo, que o polinômio $x^2 + 1$ não possui raiz em $\mathbb{R}$, porém ele possui duas raízes em $\mathbb{C}$, que é um corpo que contém o corpo dos números reais. De maneira geral, um corpo $\mathbb{L}$ é uma **extensão** de um corpo $\mathbb{K}$ se $\mathbb{K} \subset \mathbb{L}$.

Corolário 1.1. *Seja $f(x)$ um polinômio não nulo em $\mathbb{K}[x]$, então $f(x)$ tem no máximo n raízes em qualquer extensão $\mathbb{L}$ de $\mathbb{K}$.*

Note que o polinômio $x^3 - 2$ não possui raízes em $\mathbb{Q}$, possui apenas uma raiz em $\mathbb{R}$ e 3 raízes em $\mathbb{C}$. Assim, ao estendermos o corpo podemos obter mais raízes de um dado polinômio, porém esse número de raízes será sempre limitado pelo grau desse polinômio. Note também que estarmos lidando com corpos é fundamental em relação ao resultado do corolário anterior, para isso basta observar que o polinômio $x^2 + x$ possui 4 raízes no anel $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$.

Seja $\mathbb{K}$ um corpo. Como sabemos, um ideal principal de $\mathbb{K}[x]$ é da forma

$$J = \mathbb{K}[x] \cdot p(x) = \{f(x) : f(x), p(x) \in \mathbb{K}[x]\}.$$

O próximo teorema é fundamental para entender qual a forma dos ideais em $\mathbb{K}[x]$, algo que usaremos com frequência no decorrer do trabalho.

Teorema 1.5. *Todo ideal de $\mathbb{K}[x]$ é principal.*

Demonstração: Seja J um ideal de $\mathbb{K}[x]$. Se $J = \{0\}$ então J é gerado por 0. Suponha então que $J \neq \{0\}$ e tome $p(x) \neq 0 \in J$ tal que $gr(p(x))$ seja o menor possível. Note que este polinômio existe pelo princípio da boa ordenação. Se $p(x) = a$ constante e não nulo, então $1 = a^{-1} \cdot a \in J$ e assim segue direto que J é gerado por 1 e ainda, $J = \mathbb{K}[x]$. Suponha agora que $gr(p(x)) > 0$. Como $p(x) \in J$, claramente $\mathbb{K}[x] \cdot p(x) \subset J$. Agora vamos mostrar que $J \subset \mathbb{K}[x] \cdot p(x)$ e isso demonstra o teorema.

De fato, seja $f(x) \in J$. Pelo algoritmo da divisão, existem $q(x), r(x) \in \mathbb{K}[x]$ tais que

$$f(x) = q(x)p(x) + r(x)$$

onde ou $r(x) = 0$ ou $gr(r(x)) < gr(p(x))$. Agora, como $f(x), p(x) \in J$ segue que

$$r(x) = f(x) - q(x)p(x) \in J$$

e, como $p(x)$ tem o menor grau possível, é claro que $r(x) = 0$ e, portanto, temos

$$f(x) = q(x)p(x) \in \mathbb{K}[x]p(x).$$

■

Se $f(x) = a_0 + a_1x + \cdots + a_nx^n$ é um polinômio não nulo de $\mathbb{K}[x]$ tal que $a_n = 1$, dizemos que $f(x)$ é **mônico**.

Seja $\mathbb{K}$ um corpo e $\mathbb{K}[x]$ o anel de polinômios sobre $\mathbb{K}$ na indeterminada x. Agora vamos definir os polinômios que dentro da analogia de $\mathbb{K}[x]$ e $\mathbb{Z}$, fazem o papel dos números primos em $\mathbb{Z}$. Esse polinômios são chamados de polinômios irredutíveis sobre $\mathbb{K}$.

Seja $f(x) \in \mathbb{K}[x]$ tal que $gr(f(x)) \geq 1$. Tem-se que $f(x)$ é **irredutível** sobre $\mathbb{K}$ se toda vez que $f(x) = g(x)h(x)$, em que $g(x), h(x) \in \mathbb{K}[x]$, $g(x) = a$ constante ou $h(x) = b$ constante. Se $f(x)$ não for irredutível sobre $\mathbb{K}$, dizemos que $f(x)$ é **redutível** sobre $\mathbb{K}$.

Claramente temos que todo polinômio de grau 1 sobre um corpo $\mathbb{K}$ é irredutível sobre $\mathbb{K}$. Observe também que o polinômio $f(x) = x^2 + 1$ é irredutível sobre o corpo $\mathbb{R}$ mas é redutível sobre $\mathbb{C}$. Assim, um polinômio $f(x) \in \mathbb{K}$ pode ser irredutível sobre $\mathbb{K}$ e redutível sobre uma extensão $\mathbb{L}$ de $\mathbb{K}$.

Agora, vamos enunciar um resultado relacionando polinômios irredutíveis e ideais maximais que será bastante útil no estudo da teoria de códigos cíclicos.

Teorema 1.6. *Sejam $\mathbb{K}$ um corpo e $p(x) \in \mathbb{K}[x]$, então as seguintes condições são equivalentes:*

(a) $p(x)$ é irredutível sobre $\mathbb{K}$.

(b) $J = \mathbb{K}[x]p(x)$ é um ideal maximal em $\mathbb{K}[x]$.

(c) $\dfrac{\mathbb{K}[x]}{J}$ é um corpo, onde $J = \mathbb{K}[x]p(x)$.

Agora falaremos sobre o anel quociente de polinômios $\dfrac{\mathbb{K}[x]}{I}$. Afim de economizar notação, a partir de agora denotaremos um ideal $\mathbb{K}[x]p(x)$ por $\langle p(x)\rangle$. Seja $p(x)$ não nulo e considere $n = gr(p(x))$. Note que,

$$\frac{\mathbb{K}[x]}{\langle p(x)\rangle} = \{\overline{r(x)} : r(x) \in \mathbb{K}[x] \text{ com } r(x) = 0 \text{ ou } gr(r(x)) < n\}.$$

Sabemos que $\dfrac{\mathbb{K}[x]}{\langle p(x)\rangle}$ é um anel e, ainda, se $p(x)$ é irredutível então $\dfrac{\mathbb{K}[x]}{\langle p(x)\rangle}$ é um corpo. Vamos agora descrever os ideais de $\dfrac{\mathbb{K}[x]}{\langle p(x)\rangle}$.

Proposição 1.3. *Todo ideal de $\dfrac{\mathbb{K}[x]}{\langle p(x)\rangle}$ é da forma $I = \langle \overline{f(x)}\rangle$, onde $f(x)$ é um divisor de $p(x)$.*

Demonstração: Seja I um ideal de $\dfrac{\mathbb{K}[x]}{\langle p(x)\rangle}$. Considere o conjunto

$$J = \{g(x) \in \mathbb{K}[x] : \overline{g(x)} \in I\}.$$

Primeiro, vamos provar que J é um ideal de $\mathbb{K}[x]$. De fato, se $g_1(x), g_2(x) \in J$, então $\overline{g_1(x)}, \overline{g_2(x)} \in I$ e, portanto,

$$\overline{g_1(x) + g_2(x)} = \overline{g_1(x)} + \overline{g_2(x)} \in I,$$

logo, $g_1(x) + g_2(x) \in J$. Por outro lado, se $g(x) \in J$ e $h(x) \in \mathbb{K}[x]$, temos que $\overline{g(x)} \in I$, e portanto, $\overline{g(x)} \cdot \overline{h(x)} = \overline{g(x) \cdot h(x)} \in I$. Logo, $g(x)h(x) \in J$.

Sendo $J \neq \{0\}$, pois $p(x) \in J$, existe $f(x) \in \mathbb{K}[x] - \{0\}$ tal que $J = \langle f(x)\rangle$.

Como $p(x) \in J$, segue que $p(x)$ é múltiplo de $f(x)$, ou seja, $f(x)$ é um divisor de $p(x)$. Note agora que, se $I = \{\overline{(g(x))} : g(x) \in J\}$ e, como $J = \langle f(x)\rangle$, temos que

$$I = \left\{\overline{h(x)f(x)} : \overline{h(x)} \in \frac{\mathbb{K}[x]}{\langle p(x)\rangle}\right\} = \frac{\mathbb{K}[x]}{\langle p(x)\rangle}.$$

■

1.2.2 Corpos finitos

Define-se a **característica** de um corpo finito $\mathbb{K}$ como sendo o inteiro positivo

$$car(\mathbb{K}) = min\{n \in \mathbb{N} : n \cdot 1 = 0\}.$$

De maneira geral, se $\mathbb{K}$ é um corpo e existir um inteiro n positivo tal que, para todo $r \in \mathbb{K}$,

$$n \cdot r = \underbrace{r + \cdots + r}_{n \text{ vezes}} = 0,$$

então o menor desses inteiros positivos será chamado a **característica** do corpo $\mathbb{K}$. Se não existir nenhum inteiro positivo com a propriedade acima, diremos que $\mathbb{K}$ tem **característica zero**.

Se um corpo $\mathbb{F}$ é um subcorpo de um corpo $\mathbb{K}$ (a definição de subcorpo é análoga à de subanel), então $car(\mathbb{K}) = car(\mathbb{F})$. Além disso, podemos também considerar $\mathbb{K}$ como um espaço vetorial sobre $\mathbb{F}$.

Proposição 1.4. *Seja $\mathbb{F}_q$ um corpo finito, onde $q = p^n$ e p é primo. Então $car(\mathbb{K})$ é um número primo.*

Teorema 1.7. *Seja $\mathbb{K}$ um corpo finito com $car(\mathbb{K}) = p$. Então $\mathbb{K}$ contém um subcorpo isomorfo a $\mathbb{Z}_p$ (que ainda denotaremos por $\mathbb{Z}_p$). Em particular, $\mathbb{K}$ tem p^n elementos para algum número natural n.*

2 Códigos lineares

Neste capítulo iremos apresentar a classe de códigos mais utilizada na prática: os códigos lineares. Estes códigos possuem bons algoritmos do ponto de vista de codificação e decodificação e muito disso se deve ao fato da estrutura algébrica envolvida nestes códigos, que é a de espaço vetorial. Utilizaremos ferramentas de álgebra linear básica para desenvolver a teoria, evidenciando a importância e os benefícios da utilização de teoria algébrica no estudo dos códigos detectores e corretores de erros. Nosso objetivo é fazer uma síntese do assunto que será fundamental para compreensão do último capítulo sobre códigos sobre álgebras de grupo. Para isso, também introduziremos neste capítulo, uma importante subclasse dos códigos lineares, que são os códigos cíclicos. Para mais detalhes sobre os tópicos aqui apresentados, sugerimos ao leitor uma leitura dos capítulos iniciais de (HEFEZ; VILLELA, 2008).

A partir de agora, o alfabeto do código será sempre um corpo finito $\mathbb{K}$. Desta forma, para cada n natural temos um $\mathbb{K}$-espaço vetorial $\mathbb{K}^n$ de dimensão n. Seja $C \subset \mathbb{K}^n$. Dizemos que C é um **código linear** se C é um subespaço vetorial de $\mathbb{K}^n$.

Um código linear possui 3 parâmetros principais n, k e d, que são a dimensão do espaço vetorial, a dimensão do código como subespaço vetorial e a distância mínima, respectivamente. Se C tem dimensão k sobre $\mathbb{K}$, dizemos que C é um (n, k) - código linear e se C tem distância mínima d, dizemos que C é um (n, k, d) - código linear. Para a teoria de códigos, são interessantes os códigos em que k e d são relativamente grandes em relação n.

Definição 2.1. Dado $\mathbf{c} \in \mathbb{K}^n$, dizemos que o **peso** de $\mathbf{c}$ é o número inteiro

$$\omega(\mathbf{c}) = |\{i : c_i \neq \mathbf{0}\}|.$$

Em outras palavras, temos que $\omega(\mathbf{c}) = d(\mathbf{c}, \mathbf{0})$, onde d é a distância de Hamming. Além disso, o **peso de um código linear** C é o inteiro

$$\omega(C) = min\{\omega(\mathbf{c}) : \mathbf{c} \in C \setminus \{0\}\}.$$

Note que esse conjunto possui menor elmento, pois é um conjunto finito, já que $\mathbb{K}$ é um corpo finito.

Exemplo 2.1. No código do helicóptero da introdução do trabalho, as palavras $(1, 1, 0, 0, 1, 0)$ e $(1, 1, 1, 0, 0, 1)$ tem respectivamente pesos 3 e 4 e é fácil verificar que os pesos das outras palavras não nulas do código é 3. Sendo assim, o peso do código é 3.

Em um código linear C com distância mínima d, temos que $d(\mathbf{u}, \mathbf{v}) = \omega(\mathbf{u} - \mathbf{v})$, para quaisquer $\mathbf{u}, \mathbf{v} \in \mathbb{K}^n$ e, ainda, $d = \omega(C)$. Isso mostra que a distância mínima de um código linear é igual ao peso do código. Assim, é preciso efetuar $m - 1$ cálculos de distâncias em um código com m palavras para calcular sua distância mínima.

2.1 Equivalência de códigos

Quando se fala em uma classe de objetos matemáticos como os códigos, é natural se pensar sobre equivalência entre eles, isto é, objetos que possuem mesmos parâmetros. A noção de equivalência de códigos lineares é baseada no conceito de isometria linear definida a seguir.

Definição 2.2. Seja $\mathbb{K}$ um alfabeto e n natural, dizemos que uma aplicação linear $T : \mathbb{K}^n \to \mathbb{K}^n$ é uma **isometria** de $\mathbb{K}^n$ se

$$d(T(\mathbf{u}), T(\mathbf{v})) = d(\mathbf{u}, \mathbf{v}), \forall \mathbf{u}, \mathbf{v} \in \mathbb{K}^n,$$

onde d é a distância de Hamming.

Proposição 2.1. *(i) Toda isometria de $\mathbb{K}^n$ é uma bijeção de $\mathbb{K}^n$.*

(ii) A função identidade de $\mathbb{K}^n$ é uma isometria.

(iii) Se T é uma isometria de $\mathbb{K}^n$, então T^{-1} é uma isometria de $\mathbb{K}^n$.

(iv) Se T e U são isometrias de $\mathbb{K}^n$, então $T \circ U$ é uma isometria de $\mathbb{K}^n$.

Definição 2.3. Sejam C, C' códigos lineares em $\mathbb{K}^n$. Dizemos que C' é **linearmente equivalente** a C se existir uma isometria T de $\mathbb{K}^n$ tal que $T(C) = C'$.

Segue da Proposição 2.1 que a equivalência linear de códigos é uma relação de equivalência. Ou seja, é reflexiva, simétrica e transitiva. Códigos equivalentes tem os mesmos parâmetros (dimensão do espaço, dimensão do código e distância mínima).

Veremos abaixo exemplos de duas famílias importantes de isometrias.

Exemplo 2.2. Se $f : \mathbb{K} \to \mathbb{K}$ é uma bijeção linear, e i é um número tal que $1 \leq i \leq n$, então a aplicação

$$\begin{aligned} T_f^i : \mathbb{K}^n &\to \mathbb{K}^n \\ (c_1, \ldots, c_n) &\mapsto (c_1, \ldots, f(c_i), \ldots, c_n) \end{aligned}$$

é uma isometria.

Exemplo 2.3. Se π é uma bijeção do conjunto $\{1, \ldots, n\}$ nele prório, também chamada permutação de $\{1, \ldots, n\}$, então a aplicação permutação de coordenadas

$$\begin{array}{rcl} T_\pi : \mathbb{K}^n & \to & \mathbb{K}^n \\ (c_1, \ldots, c_n) & \mapsto & (c_{\pi(1)}, \ldots, c_{\pi(n)}) \end{array}$$

é uma isometria.

O teorema a seguir nos dá uma caracterização das isometrias de $\mathbb{K}^n$ e, portanto, nos dá uma maneira de obter códigos equivalentes.

Teorema 2.1. *Seja $T : \mathbb{K}^n \to \mathbb{K}^n$ uma isometria. Então existem uma permutação π de $\{1, \ldots, n\}$ e bijeções lineares f_i de $\mathbb{K}$, $i = 1, \ldots, n$ tais que*

$$T = T_\pi \circ T^1_{f_1} \circ \cdots \circ T^n_{f_n}.$$

Corolário 2.1. *Sejam C e C' códigos lineares em $\mathbb{K}^n$. Então C e C' são linearmente equivalentes se, e somente se, existem uma permutação π de $\{1, \ldots, n\}$ e bijeções lineares $f_1, \ldots, f_n$ de $\mathbb{K}$ tais que*

$$C' = \{(f_{\pi(1)}(c_{\pi(1)}), \ldots, f_{\pi(n)}(c_{\pi(n)})) : (c_1, \ldots, c_n) \in C\}.$$

Observe que se $f : \mathbb{K} \to \mathbb{K}$ é linear, existe $c \in \mathbb{K}$ tal que

$$f(x) = cx, \text{ para todo } x \in \mathbb{K}.$$

Com isso, C é linearmente equivalente a C' em $\mathbb{K}^n$ se, e somente se,

$$C' = \{(c_1(x_{\pi(1)}), \ldots, c_n(x_{\pi(n)})) : (x_1, \ldots, x_n) \in C, c_i \in \mathbb{K}\}.$$

Isso equivale a dizer que dois códigos lineares são linearmente equivalentes se, e somente se, cada um deles pode ser obtido do outro mediante uma sequência de operações do tipo:

- Multiplicação dos elementos numa dada posição fixa por um escalar não nulo em todas as palavras.
- Permutação das posições de todas as palavras do código, mediante uma permutação fixa de $\{1, \ldots, n\}$.

2.2 Matriz Geradora de um código

O objetivo dessa seção é mostrar as vantagens que obtemos ao mesclar códigos corretores de erros com estruturas algébricas, em particular a estrutura dos espaços vetoriais.

Seja $\mathcal{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ uma base de um código linear C e considere a matriz G a seguir.

$$G = \begin{pmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_k \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ \vdots & \vdots & & \vdots \\ v_{k1} & v_{k2} & \ldots & v_{kn} \end{pmatrix}.$$

G é chamada de **matriz geradora** de C associada à base $\mathcal{B}$, e sua importância será evidenciada a seguir.

Considere a transformação linear definida por

$$\begin{aligned} T : \mathbb{K}^k &\rightarrow \mathbb{K}^n \\ \mathbf{c} &\mapsto \mathbf{c}G. \end{aligned}$$

Se $\mathbf{c} = (c_1, \ldots, c_k)$, temos que

$$T(\mathbf{c}) = \mathbf{c}G = c_1\mathbf{v}_1 + \cdots + c_k\mathbf{v}_k.$$

Logo $T(\mathbb{K}^k) = C$. Daí, podemos considerar $\mathbb{K}^k$ como o **código da fonte**, C o **código do canal** e T uma **codificação**.

Lembramos que G não é univocamente determinada, pois depende da escolha da base. Observe ainda, que uma base de um espaço vetorial pode ser obtida de uma outra qualquer através de sequências de operações do tipo:

- Permutação de dois elementos da base;
- Multiplicação de um elemento da base por um escalar não nulo;
- Substituição de um elemento da base por ele mesmo somado a um múltiplo escalar de outro elemento da base.

Segue, então que duas matrizes geradoras de um mesmo código podem ser obtidas uma da outra por sequências de operações do tipo:

- (L1) Permutação de duas linhas;
- (L2) Multiplicação de uma linha por um escalar não nulo;
- (L3) Adição de um múltiplo escalar de uma linha a outra.

Com isso, dada uma matriz G qualquer cujas linhas são linearmente independentes, podemos construir um código linear C como imagem de uma transformação representada por essa matriz G.

Veja agora um exemplo da utilização de uma matriz geradora.

Exemplo 2.4. Seja o corpo finito com 2 elmentos $\mathbb{F}_2$ o alfabeto de um código linear C, e considere a seguinte transformação linear

$$\begin{aligned} T : \mathbb{F}_2^3 &\rightarrow \mathbb{F}_2^5 \\ \mathbf{c} &\mapsto \mathbf{c}G. \end{aligned}$$

Seja $\mathcal{B} = \{(1,0,1,0,1),(1,1,0,1,0),(1,1,1,1,1)\} \subset \mathbb{F}_2^5$ uma base de C. Desta forma,

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

é uma matriz geradora de um código C em $\mathbb{F}_2^5$. Fazendo $T((1,1,0))$, obtemos $(0,1,1,1,1)$ como codificação.

Agora, suponha que se queira decodificar a palavra $(1,0,0,0,0)$ do código de canal, isto é, encontrar a palavra do código da fonte à qual ela corresponde por meio de T. Basta resolver o sistema linear

$$(c_1, c_2, c_3)G = (1,0,0,0,0),$$

ou seja,

$$\begin{cases} c_1 + c_2 + c_3 = 1 \\ c_2 + c_3 = 0 \\ c_1 + c_3 = 0 \\ c_2 + c_3 = 0 \\ c_1 + c_3 = 0 \end{cases}$$

cuja solução é $c_1 = 1, c_2 = 1$ e $c_3 = 1$.

Para utilizar a matriz G na codificação e decodificação de palavras do código, será preciso resolver um sistema de equações que, em geral, dada uma matriz G mais complexa que essa do exemplo, pode dar muito trabalho, é nesse sentido que damos a próxima definição.

Definição 2.4. Seja G uma matriz geradora de um código linear C. Dizemos que G está na **forma padrão** se

$$G = (Id_k \mid A),$$

onde Id_k é a matriz identidade $k \times k$ e A uma matriz $k \times (n-k)$.

Dado um código linear C, nem sempre conseguimos encontrar uma matriz geradora de C na forma padrão. Contudo, se G é uma matriz geradora de C, podemos permutar colunas de G, obtendo uma matriz G' que é a matriz geradora na forma padrão de um código C' equivalente a C.

Teorema 2.2. *Dado um código linear C, existe um código C' equivalente a C que possui matriz geradora na forma padrão.*

2.3 Códigos Duais

Definiremos nesta seção o código dual de um código linear C. Esses códigos são fundamentais no que diz respeito à verificação se determinada palavra em $\mathbb{K}^n$ pertence ou não ao código C.

Dados $\mathbf{u} = (u_1, \ldots, u_n)$ e $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{K}^n$, define-se o produto interno de $\mathbf{u}$ e $\mathbf{v}$ por

$$\mathbf{u} \cdot \mathbf{v} = u_1 v_1 + \cdots + u_n v_n.$$

Além disso, o produto interno satisfaz as propriedades de simetria

$$\mathbf{u} \cdot \mathbf{v} = \mathbf{v} \cdot \mathbf{u}$$

e bilinearidade

$$(\mathbf{u} + \lambda \mathbf{w}) \cdot \mathbf{v} = \mathbf{u} \cdot \mathbf{v} + \lambda(\mathbf{w} \cdot \mathbf{u})$$

para todo $\lambda \in \mathbb{K}$.

Seja $C \subset \mathbb{K}^n$ um código linear. Define-se o conjunto ortogonal a C em $\mathbb{K}^n$ por

$$C^{\perp} = \{\mathbf{v} \in \mathbb{K}^n : \mathbf{u} \cdot \mathbf{v} = 0, \forall \mathbf{u} \in C\}.$$

O conjunto $C^{\perp}$ é um subespaço vetorial de $\mathbb{K}^n$ e, portanto, também é um código linear que chamaremos de **código dual** de C.

Sejam C um (n, k)-código com matriz geradora G e $\mathbf{v} \in C^{\perp}$. Então $\mathbf{v} \cdot \mathbf{c} = \mathbf{0}$, para todo $\mathbf{c} \in C$. Logo $\mathbf{v}$ é ortogonal a todos os elementos de uma base de C, o que equivale a dizer que $G\mathbf{v}^t = 0$, já que a matriz G é formada pelos vetores de uma base de C. Assim podemos definir o código dual $C^{\perp}$ da seguinte forma,

$$C^{\perp} = \{\mathbf{v} \in \mathbb{K}^n : G\mathbf{v}^t = \mathbf{0}\}.$$

Os resultados a seguir, que encerram essa seção, são obtidos através de aplicações de conceitos básicos de álgebra linear.

Proposição 2.2. *Seja $C \subset \mathbb{K}^n$ um código de dimensão k com matriz geradora $G = (Id_k \mid A)$ na forma padrão. Então*

(i) $\dim C^{\perp} = n - k$;

(ii) $H = (-A^t | Id_{n-k})$ *é uma matriz geradora de* C;

(iii) $(C^{\perp})^{\perp} = C$.

Proposição 2.3. *Sejam* C *e* D *dois códigos lineares em* $\mathbb{K}^n$. *Se* C *e* D *são linearmente equivalentes, então* $C^{\perp}$ *e* $D^{\perp}$ *também são linearmente equivalentes.*

Lema 2.1. *Seja* $C \subset \mathbb{K}^n$ *um código linear de dimensão* k *com matriz geradora* G. *Uma matriz* H *de ordem* $(n-k) \times n$ *com coeficiente em* $\mathbb{K}$ *e linhas linearmente independente, é uma matriz geradora de* $C^{\perp}$ *se, e somente se,*

$$G \cdot H^t = \mathbf{0}.$$

Ou seja, todos os vetores do subespaço gerado pelas linhas de H estão em $C^{\perp}$. Por outro lado, esse subespaço tem a mesma dimensão de $C^{\perp}$. Assim, $G \cdot H^t = \mathbf{0}$ se, e somente se, $C^{\perp}$ é gerado pelas linhas de H.

A proposição a seguir nos mostra como identificar se um elemento de $\mathbb{K}^n$ pertence ou não a um código $C \subset \mathbb{K}^n$.

Proposição 2.4. *Sejam* $C \subset \mathbb{K}^n$ *um código linear tal que* $C^{\perp}$ *tem matriz geradora* H *e* $\mathbf{v} \in \mathbb{K}^n$. *Então*

$$\mathbf{v} \in C \iff H\mathbf{v}^t = \mathbf{0}.$$

A proposição acima nos permite caracterizar os elementos de um código C por uma condição de anulamento. A matriz geradora H de $C^{\perp}$ é chamda de **matriz teste de paridade** de C.

Com isso, os elementos de C ficam determinados por uma condição de anulamento, tendo um custo computacional baixo, pois basta determinar se $H\mathbf{v}^t$ é o vetor nulo de $\mathbb{K}^n$ para que $\mathbf{v}$ pertença a C.

2.4 Códigos cíclicos

Esta seção será dedicada ao objeto central deste trabalho, os códigos cíclicos, que são códigos lineares com algumas propriedades adicionais. Os códigos cíclicos possuem uma rica estrutura, podendo ser gerados não só a partir de matrizes geradoras, mas também por polinômios geradores, o que reduz significativamente os custos para implementar o código computacionalmente.

Considere a aplicação

$$\begin{aligned} \sigma : \mathbb{K}^n &\to \mathbb{K}^n \\ (c_0, c_1, \ldots, c_{n-2}, c_{n-1}) &\mapsto (c_{n-1}, c_0, c_1 \ldots, c_{n-2}). \end{aligned}$$

Chamaremos σ de **troca cíclica**. Um código linear $C \subset \mathbb{K}^n$ é um ***código cíclico*** se $\sigma(c) \in C$ para todo $c \in C$, isto é, se $c = (c_0, c_1, \ldots, c_{n-1}) \in C$, então $c' = (c_{n-1}, c_0, \ldots, c_{n-2}) \in C$.

Exemplo 2.5. O código $C = \{(0,0,0,0), (1,0,1,0), (0,1,0,1), (1,1,1,1)\}$ é cíclico. Note que C é um subespaço vetorial de $\mathbb{F}_2^4$ e tem os seguintes parâmetros: comprimento 4, dimensão 2 e distância mínima 2.

Para trabalhar com códigos cíclicos, o que faremos é dar a eles uma estrutura de anel, além da estrutura de espaço vetorial de $\mathbb{K}^n$, pois a partir disso poderemos fazer uso das propriedades dessa estrutura algébrica, o que será de grande ajuda, como veremos mais adiante.

Seja $\langle x^n - 1\rangle$ o ideal de $\mathbb{K}[x]$ gerado por $x^n - 1$ e defina R_n como o anel quociente dado por

$$R_n = \frac{\mathbb{K}[x]}{\langle x^n - 1\rangle}.$$

Assim, se $\overline{f(x)} \in R_n$, então

$$\overline{f(x)} = \{f(x) + g(x)(x^n - 1) : g(x) \in \mathbb{K}[x]\}$$

e as operações de adição e multiplicação são definidas respectivamente da seguinte maneira:

$$\overline{f(x)} + \overline{g(x)} = \overline{f(x) + g(x)}$$
$$\overline{f(x)} \cdot \overline{g(x)} = \overline{f(x) \cdot g(x)}$$

para quaisquer $\overline{f(x)}, \overline{g(x)} \in R_n$.

Temos também que R_n munido da multiplicação por escalar $\lambda \in \mathbb{K}$, dada por

$$\lambda\overline{f(x)} = \overline{\lambda f(x)}, \quad \forall\ \overline{f(x)} \in R_n$$

é um $\mathbb{K}$-espaço vetorial de dimensão n com base $\mathcal{B} = \left\{1, \overline{x}, \ldots, \overline{x^{n-1}}\right\}$ e, então, R_n é isomorfo a $\mathbb{K}^n$ e usaremos aqui o seguinte isomorfismo linear:

$$\begin{aligned} \nu : \mathbb{K}^n &\to R_n \\ (c_0, c_1, \ldots, c_{n-1}) &\mapsto \overline{c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}}. \end{aligned}$$

Até aqui, vimos que R_n possui as estruturas de anel e espaço vetorial e que é isomorfo a $\mathbb{K}^n$, o que significa que todo código linear $C \subset \mathbb{K}^n$ pode ser visto em R_n através do isomorfismo ν, o que nos permite usar ferramentas de anéis na busca de melhores algoritmos de codificação e decodificação.

2.4.1 Matrizes geradoras e teste de paridade de um código cíclico

Nesta seção, nosso objetivo é encontrar matrizes geradoras e matrizes teste de paridade para códigos cíclicos, mas primeiro vamos caracterizar estes códigos em R_n. Note que a troca cíclica em R_n é dada, através de ν, pela multiplicação de $\overline{f(x)}$ por $\overline{x}$. De fato, dado $\overline{f(x)} = \overline{c_0 + c_1x + \cdots + c_{n-2}x^{n-2} + c_{n-1}x^{n-1}} \in R_n$, temos que

$$\begin{aligned}
\overline{f(x)} \cdot \overline{x} &= \overline{f(x) \cdot x} \\
&= \overline{(c_0 + c_1x + \cdots + c_{n-2}x^{n-2} + c_{n-1}x^{n-1}) \cdot x} \\
&= \overline{c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1} + c_{n-1}x^n} \\
&= \overline{c_{n-1} + c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1}}.
\end{aligned}$$

O lema e o teorema a seguir nos dão uma caracterização precisa dos códigos cíclicos em R_n.

Lema 2.2. *Seja V um subespaço vetorial de R_n. Então, V é um ideal de R_n se, e somente se, V é fechado pela multiplicação por $\overline{x}$.*

Demonstração: Se V é um ideal de R_n, é direto da definição de ideais que $\overline{x} \cdot \overline{f(x)} \in V$, para todo $\overline{f(x)} \in V$. Por outro lado, se V é fechado pela multiplicação por $\overline{x}$, basta mostrar que $\overline{g(x)} \cdot \overline{f(x)} \in V$ para quaisquer $\overline{g(x)} \in R_n, \overline{f(x)} \in V$.

De fato, como V é um subespaço vetorial de R_n, temos que $a\overline{f(x)} \in V$, para quaisquer $a \in \mathbb{K}$ e $\overline{f(x)} \in V$. Como por hipótese,

$$\overline{xf(x)} = \overline{x} \cdot \overline{f(x)} \in V,$$

então

$$\overline{x^2f(x)} = \overline{x} \cdot \overline{xf(x)} \in V.$$

Obtemos, por indução, que para todo $m \in \mathbb{N}$ temos que

$$\overline{x^mf(x)} = \overline{x^m} \cdot \overline{f(x)} \in V.$$

Daí, escrevendo

$$\overline{g(x)} = \overline{a_0 + a_1x + \cdots + a_{n-1}x^{n-1}},$$

temos

$$\overline{g(x)} \cdot \overline{f(x)} = a_0\overline{f(x)} + a_1\overline{x} \cdot \overline{f(x)} + \cdots + a_{n-1}\overline{x^{n-1}} \cdot \overline{f(x)} \in V,$$

pois V é um subespaço vetorial e cada parcela da última expressão pertence a V. ∎

Teorema 2.3. *Um subespaço C de $\mathbb{K}^n$ é um código cíclico se, e somente se, $\nu(C)$ é um ideal de R_n.*

Demonstração: Seja C um subespaço vetorial de $\mathbb{K}^n$. Suponha que $\nu(C)$ é um ideal de R_n. Daí, pelo Lema 2.2, $\nu(C)$ é fechado pela multiplicação por $\overline{x}$ e, portanto, $\nu^{-1}(\nu(C)) = C$ é um código cíclico.

Por outro lado, se C é um código cíclico, então vale a troca cíclica para $\nu(C)$ em R_n, isto é, $\overline{x} \cdot \overline{f(x)} \in \nu(C)$ para todo $\overline{f(x)} \in \nu(C)$. Logo, novamente pelo Lema 2.2 temos que $\nu(C)$ é um ideal de R_n. ■

Observe que para verificar se um subespaço vetorial C de $\mathbb{K}^n$ é um código cíclico sem a utilização do Teorema 2.3, seria preciso verificar se todas as trocas cíclicas pertencem a C, o que poderia ser muito trabalhoso. Agora, é suficiente verificar se $\nu(C)$ é um ideal de R_n.

Vimos na Proposição 1.3 que um ideal no anel quociente R_n é da forma $\langle\overline{p(x)}\rangle$, onde $p(x)$ é divisor de $x^n - 1$. Então a partir de agora, $g(x)$ será sempre um divisor de $x^n - 1$ e ainda, denotaremos

$$h(x) = \frac{x^n - 1}{g(x)}.$$

Teorema 2.4. *Seja $I = \left\langle\overline{g(x)}\right\rangle$ um ideal de R_n. Se $g(x)$ tem grau s, então temos que $\mathcal{B} = \left\{\overline{g(x)}, \overline{xg(x)}, \overline{x^2g(x)}, \ldots, \overline{x^{n-s-1}g(x)}\right\}$ é uma base de I como espaço vetorial sobre $\mathbb{K}$.*

Demonstração: Note que, se

$$a_0\overline{g(x)} + a_1\overline{x} \cdot \overline{g(x)} + \cdots + a_{n-s-1}\overline{x^{n-s-1}} \cdot \overline{g(x)} = 0,$$

temos,

$$\left[a_0 + a_1\overline{x} + \cdots + a_{n-s-1}\overline{x^{n-s-1}}\right] \overline{g(x)} = 0.$$

Assim, pelo algoritmo da divisão, existe $d(x) \in \mathbb{K}[x]$ tal que

$$\left[a_0 + a_1x + \cdots + a_{n-s-1}x^{n-s-1}\right] g(x) = d(x)(x^n - 1),$$

isto é,

$$a_0 + a_1x + \cdots + a_{n-s-1}x^{n-s-1} = d(x)h(x).$$

Como o grau de $h(x)$ é $n - s$, temos então que

$$a_0 + a_1x + \cdots + a_{n-s-1}x^{n-s-1} = 0$$

e, portanto, $a_0 = a_1 = \cdots = a_{n-s-1} = 0$. Além disso, dado $\overline{f(x)} \in I$, temos que

$$f(x) \equiv d(x) \cdot g(x) \mod (x^n - 1).$$

Pelo algoritmo da divisão, existem $d(x)$,$r(x) \in \mathbb{K}[x]$ tais que

$$d(x) = h(x) \cdot c(x) + r(x),$$

com $r(x) = a_0 + a_1 x + \cdots a_{n-s-1}x^{n-s-1}$. Daí,

$$f(x) \equiv d(x) \cdot g(x) \equiv c(x) \cdot h(x) \cdot g(x) + r(x) \cdot g(x) \mod (x^n - 1),$$

e logo,

$$f(x) \equiv c(x)(x^n - 1) + r(x) \cdot g(x) \equiv r(x) \cdot g(x) \mod (x^n - 1).$$

Desta forma,

$$\overline{f(x)} = a_0\overline{g(x)} + a_1\overline{xg(x)} + \cdots + a_{n-s-1}\overline{x^{n-s-1}}.$$

■

Uma consequência direta do Teorema 2.4 é que se $I = \left\langle \overline{g(x)} \right\rangle$ é um ideal gerado como $\mathbb{K}$-espaço vetorial pela base $\mathcal{B}$, então fazendo $\mathbf{v} = \nu^{-1}\left(\overline{g(x)}\right)$, temos que C é gerado por $\{\mathbf{v}, \sigma(\mathbf{v}), \sigma^2(\mathbf{v}), \ldots, \sigma^{n-s-1}(\mathbf{v})\}$.

Corolário 2.2. *Seja $g(x)$ um polinômio divisor de $x^n - 1$ de grau s. Se $I = \left\langle \overline{g(x)} \right\rangle$ é um ideal de R_n, então*

$$\dim_{\mathbb{K}} I = n - s,$$

e o código $C = \nu^{-1}(I)$ tem matriz geradora dada por

$$G = \begin{pmatrix} \nu^{-1}\left(\overline{g(x)}\right) \\ \nu^{-1}\left(\overline{xg(x)}\right) \\ \vdots \\ \nu^{-1}\left(\overline{x^{n-s-1}g(x)}\right) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \ldots & g_s & 0 & \ldots & 0 \\ 0 & g_0 & g_1 & \ldots & g_s & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \ldots & 0 & \ldots & g_0 & \ldots & g_s \end{pmatrix}$$

Demonstração: Recorde que as linhas de uma matriz geradora de um código linear C são dadas pelos vetores da base. Neste caso, temos que $\mathcal{B} = \left\{\overline{g(x)}, \overline{xg(x)}, \overline{x^2g(x)}, \ldots, \overline{x^{n-s-1}g(x)}\right\}$ é uma base para o ideal $I = \left\langle \overline{g(x)} \right\rangle$ de R_n e, utilizando a imagem inversa do isomorfimo ν, obtemos uma base para o código em $\mathbb{K}^n$. ■

Seja $p(x) = p_0 + p_1 x + \cdots + p_t x^t$ um polinômio que divide $x^n - 1$. Chamaremos de **polinômio recíproco** de $p(x)$, o polinômio

$$p^*(x) = x^t f(x^{-1}) = p_t + p_{t-1}x + \cdots + p_0 x^t. \tag{2.1}$$

Este polinômio também divide $x^n - 1$ e, portanto, é gerador de algum código cíclico. Quando consideramos o código cíclico gerado pelo polinômio recíproco de $h(x) = \frac{x^n-1}{g(x)}$ teremos um auxílio para encontrar uma matriz teste de paridade para o código cíclico C gerado por $g(x)$, como veremos no teorema a seguir.

Teorema 2.5. *Seja $C = \nu^{-1}(I)$ um código cíclico, onde $I = \left\langle \overline{g(x)} \right\rangle$ é um ideal de R_n. Daí, $C^\perp$ é cíclico e $C^\perp = \nu^{-1}(J)$, onde J é o ideal de R_n gerado por $\overline{h^*(x)}$. Isto é, $J = \left\langle \overline{h^*(x)} \right\rangle$.*

Demonstração: Sejam $g(x) = g_0 + g_1x + \cdots + g_sx^s$ e $h(x) = h_0 + h_1x + \cdots + h_{n-s}x^{n-s}$. Note que o grau de $h(x)$ é $n - s$ e, portanto, $h_{n-s} \neq 0$. Considere as matrizes G e H a seguir:

$$G = \begin{pmatrix} g_0 & g_1 & \dots & g_s & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_s & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \dots & 0 & \dots & g_0 & \dots & g_s \end{pmatrix} \text{ e } H = \begin{pmatrix} h_{n-s} & h_{n-s-1} & \dots & h_0 & 0 & \dots & 0 \\ 0 & h_{n-s} & h_{n-s-1} & \dots & h_0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \dots & 0 & \dots & h_{n-s} & \dots & h_0 \end{pmatrix}.$$

É fácil ver que as linhas de H são linearmente independentes. Seja $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ a base canônica de $\mathbb{K}^n$. Assim, a i-ésima linha de G é dada por

$$G_i = g_0\mathbf{e}_i + g_1\mathbf{e}_{i+1} + \cdots + g_s\mathbf{e}_{i+s},\ 1 \leq i \leq n - s,$$

e a j-ésima coluna de H^t é dada por

$$H_j = h_{n-s}\mathbf{e}_j + h_{n-s-1}\mathbf{e}_{j+1} + \cdots + h_0\mathbf{e}_{j+n-s},\ 1 \leq j \leq s.$$

Suponha que $i \leq j$. Daí, o produto interno de G_i por H_j é dado por

$$g_{j-i}h_{n-s} + g_{j-i+1}h_{n-s-1} + \cdots + g_0h_{j-i},$$

com $(j - i) \in \{0, \dots, s - 1\}$. Note que a soma acima é o coeficiente de $x^{n-s+j-i}$ no produto $g(x)h(x) = x^n - 1$ e, como $1 \leq n - s + j - i \leq n - 1$, temos que esse coeficiente obrigatoriamente deve ser 0. O resultado é análogo se $j \leq i$. ∎

Como $h^*(x)$ tem grau $n - s$ e divide $x^n - 1$, com o Corolário 2.2 e o Teorema 2.5, podemos afirmar que o código $C^\perp$ tem matriz geradora dada por

$$H = \begin{pmatrix} \nu^{-1}\left(\overline{h^*(x)}\right) \\ \nu^{-1}\left(\overline{xh^*(x)}\right) \\ \vdots \\ \nu^{-1}\left(\overline{x^{s-1}h^*(x)}\right) \end{pmatrix} = \begin{pmatrix} h_{n-s} & h_{n-s-1} & \dots & h_0 & 0 & \dots & 0 \\ 0 & h_{n-s} & h_{n-s-1} & \dots & h_0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \dots & 0 & \dots & h_{n-s} & \dots & h_0 \end{pmatrix}$$

e, portanto, H é uma matriz teste de paridade para C.

2.4.2 Codificação em Códigos Cíclicos

Nessa seção mostraremos como encontrar uma matriz geradora na forma padrão e ainda, um algoritmo de codificação para esses códigos.

Sejam $C \subset \mathbb{K}^n$ um código cíclico e considere o isomorfismo de $\mathbb{K}$-espaços vetoriais, onde $\mathbb{K}[x]_{s-1}$ é o espaço vetorial dos polinômios de grau no máximo $s-1$ a seguir:

$$\begin{array}{rcl} \mu : \mathbb{K}^s & \to & \mathbb{K}[x]_{s-1} \subset \mathbb{K}[x] \\ (c_0, c_1, \ldots, c_{s-1}) & \mapsto & \sum_{i=0}^{s-1} c_i x^i. \end{array}$$

Teorema 2.6. *Seja C um código cíclico. Suponha $C = \nu^{-1}(I)$, onde $I = \left\langle \overline{g(x)} \right\rangle$, com $g(x)$ divisor de $x^n - 1$. Seja R a matriz $(n-s) \times s$ cuja i-ésima linha é*

$$R(i) = -\mu^{-1}(r_i(x)),$$

onde $r_i(x)$ é o resto da divisão de x^{s-1+i} por $g(x)$. Então a matriz $(R \mid Id_{n-s})$ é uma matriz geradora de C.

Demonstração: Sejam $q_i(x)$ e $r_i(x)$ o quociente e o resto da divisão de x^{s-1+i} por $g(x)$, respectivamente. Desta forma,

$$x^{s-1+i} = g(x)q_i(x) + r_i(x),$$

onde $r_i(x) = 0$ ou $r_i(x)$ tem grau menor ou igual a $s-1$. Sendo assim, $\overline{x^{s-1+i} - r_i(x)} \in I$, e esses vetores para $i = 1, \ldots, n-s$ são linearmente independentes sobre $\mathbb{K}$. Como $\nu^{-1}\left(\overline{x^{s-1+i} - r_i(x)}\right) = \mathbf{e}_{s-1+i} - \mu^{-1}(r_i(x))$, onde $\mathbf{e}$ é vetor da base canônica de $\mathbb{K}^n$, temos que a matriz

$$\begin{pmatrix} -\mu^{-1}(r_1(x)) & 1 & 0 & \ldots & 0 \\ -\mu^{-1}(r_2(x)) & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & & \\ -\mu^{-1}(r_{n-s}(x)) & 0 & 0 & \ldots & 1 \end{pmatrix}$$

é uma matriz geradora de C e então $(Id_{n-s} \mid R)$ é uma matriz geradora de C na forma padrão. ∎

Agora, veremos o algoritmo de codificação. Dado $(c_0, c_1, \ldots, c_{n-s}) \in \mathbb{K}^{n-s}$, esse vetor pode ser codificado como elemento de C como se segue:

$$(c_0, c_1, \ldots, c_{n-s})(R \mid Id_{n-s}) = (b_0, \ldots, b_{s-1}, c_1, \ldots, c_{n-s}),$$

onde

$$\begin{array}{rcl} (b_0, \ldots, b_{s-1}) & = & -c_1\mu^{-1}(r_1(x)) - \cdots - c_{n-s}\mu^{-1}(r_{n-s}(x)) \\ & = & -\mu^{-1}(c_1 r_1(x) + \cdots + (c_{n-s}r_{n-s}(x)) \\ & = & -\mu^{-1}\left(\sum_{i=1}^{n-s} a_i r_i(x)\right) \end{array}$$

Veja um exemplo para ilustrar melhor a ideia.

Exemplo 2.6. Considere o polinômio $x^7 - 1$ sobre $\mathbb{F}_2$. A fatoração de $x^7 - 1$ é dada por

$$x^7 - 1 = (1 + x)(1 + x + x^3)(1 + x^2 + x^3).$$

Considere o código $C \subset \mathbb{F}_2^7$ gerado por $g(x) = 1 + x + x^3$. Note que a dimensão do código é 4. Agora, vamos determinar uma matriz geradora desse código na forma padrão:

$$\begin{aligned} x^3 &= (x^3 + x + 1) + (x + 1) \\ x^4 &= (x^3 + x + 1)x + (x^2 + x) \\ x^5 &= (x^3 + x + 1)(x^2 + 1) + (x^2 + x + 1) \\ x^6 &= (x^3 + x + 1)(x^3 + x + 1) + (x^2 + 1). \end{aligned}$$

Sendo assim, pelo Teorema 2.6, uma matriz geradora de C é dada por

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Suponha que seja dado um vetor $(a_1, a_2, a_3, a_4) \in \mathbb{F}_2^4$, do código da fonte. Digamos, por exemplo, o vetor $(1, 1, 1, 0)$. Assim, de acordo com a discussão acima, a codificação desse vetor é

$$(b_0, b_1, b_2, 1, 1, 1, 0),$$

onde b_0, b_1 e b_2 são os coeficientes do polinômio

$$1 \cdot (1 + x) + 1 \cdot (x + x^2) + 1 \cdot (1 + x + x^2) + 0 \cdot (1 + x^2) = 0 + x + 0 \cdot x^2.$$

Portanto, a codificação de $(1, 1, 1, 0)$ é $(0, 1, 0, 1, 1, 1, 0)$.

3 Álgebras de grupo

Entre as bases que sustentam a álgebra, há dois assuntos que se destacam: a teoria de grupos e a teoria de anéis e álgebras, embora existam outros tópicos também importantes. No século XX, começou a se consolidar uma nova área de pesquisa em álgebra, apoiada nesses dois tópicos, que veio a ser conhecida como teoria dos anéis de grupo. A partir da segunda metade do século XX que a teoria começou a fixar suas principais questões e pervadir outras áreas da álgebra e mesmo outros campos das matemática. Um anel de grupo é uma estrutura híbrida entre as teorias de grupo e de anéis, que é definida como um módulo livremente gerado sobre um grupo com coeficientes em um anel associativo com unidade. A relevância da estrutura é que, entre outras coisas, é possível lançar-se mão das poderosas ferramentas de ambas as teorias, de grupos e de anéis, em seu estudo. Muitas são as suas questões centrais e as soluções dessas questões têm iluminado problemas profundos em outros campos da matemática. Entre essas questões, destacamos o problema do isomorfismo com implicações importantes em teoria de grupos. Curiosamente, à medida que a teoria de anéis de grupo se desenvolvia, pelas mãos de G. Higman, S. D. Berman, H. Zassenhaus, D. S. Passman, S. K. Sehgal e outros, a partir da segunda metade do século XX, a teoria de códigos também se firmava, tendo como desbravador C. E. Shannon. No desenvolver da teoria de códigos, notou-se que a utilização de estruturas algébricas traria um ganho enorme. Neste contexto, a utilização de anéis de grupo geram o que chamamos de códigos de grupo. Iremos tratar desse assunto no próximo capítulo. Neste capítulo, iremos desenvolver os conceitos básicos da teoria de anéis de grupos. Para isso, começaremos com um breve resumo da teoria de módulos. A teoria de módulos por si só é uma importante área de pesquisa em matemática e é repleta de importantes resultados, como o Teorema de Wedderburn-Artin. Porém, para não perdemos o foco do nosso trabalho, este resultado, assim como a maioria dos resultados sobre módulos serão apenas enunciados e utilizados. Nosso foco aqui, é dar o máximo de elementos possíveis sobre a teoria de anéis de grupo para que os utilizemos na compreensão dos códigos de grupo, em especial, os códigos de grupo cíclicos. Para mais detalhes sobre módulos ou anéis de grupo, inclusive para as demonstrações omitidas aqui, sugerimos (MILIES; SEHGAL, 2002).

3.1 Módulos

Seja R um anel com unidade 1. Diz-se que um conjunto não-vazio M é um **módulo à esquerda** sobre R (ou um R-**módulo à esquerda**) se temos definida em M uma operação, que indicaremos por $+$, e uma lei de composição externa que a cada

par $(a, m) \in R \times M$ associa um elemento $am \in M$ tal que, para quaisquer $a, b \in R$ e $m, m_1, m_2 \in M$, verifica-se:

(i) $(m + m_1) + m_2 = m + (m_1 + m_2)$;

(ii) Existe um elemento $0 \in M$ tal que $m + 0 = m = 0 + m$;

(iii) Existe um elemento em M, que denotaremos por $-m$, tal que $m + (-m) = 0$;

(iv) $m_1 + m_2 = m_2 + m_1$;

(v) $(a + b)m = am + bm$;

(vi) $a(m_1 + m_2) = am_1 + am_2$;

(vii) $a(bm) = (ab)m$;

(viii) $1m = m$.

De forma análoga pode-se definir a noção de R-**módulo à direita**, considerando a multiplicação à direita por elementos do anel.

Note que, poderíamos substituir as 4 primeiras propriedades da definição acima pela exigência que M deve ser um grupo abeliano. E ainda, se R for um corpo, então a definição de R-módulo coincide com a de um R-espaço vetorial. Por essa razão, a estrutura de módulos é vista como uma generalização dos espaços vetoriais.

Seja I um ideal à esquerda de um anel R. Então I admite uma estrutura de R-módulo com soma induzida pela soma de R e a aplicação $R \times I \mapsto I$ dada pela multiplicação (à esquerda) por elementos de R. Em particular, um anel é sempre um módulo sobre si mesmo. E quando queremos nos referir a R como um módulo sobre si mesmo à esquerda ou à direita usamos, respectivamente, as notações ${}_RR$ e R_R.

É importante ressaltar que podemos definir módulos para anéis que não possuem unidade. Contudo, no que segue, quando falarmos em anéis, estaremos considerando apenas anéis com unidade.

Definição 3.1. Seja R um anel comutativo. Um R-módulo A é dito uma R-**álgebra** se existe uma multiplicação, definida em A, tal que, com a adição dada em A e esta multiplicação, A é um anel e tal que as seguintes condições são satisfeitas:

Definição 3.2. Sejam M um R-módulo e N um subconjunto de M. Dizemos que N é um R-**submódulo** de M (ou simplesmente, um **submódulo**) se

(i) $N \neq \varnothing$ e para quaisquer $m, n \in N$ tem-se $m - n \in N$.

(ii) Para todo $r \in R$ e todo $n \in N$, temos $rn \in N$.

Observação 3.1. *Se considerarmos um anel R como um R-módulo à esquerda sobre si mesmo, então os submódulos de ${}_RR$ são seus ideais à esquerda.*

Assim como na teoria de anéis, todo R-módulo M não vazio contém pelo menos dois submódulos, M e $\{0\}$, que são os **triviais**. Um submódulo diferente dos triviais é um submódulo **próprio**. Um R-módulo não vazio e diferente de $\{0\}$ que não possui submódulos próprios é chamado de **módulo simples**.

Analogamente à teoria de anéis e grupos, uma aplicação $f : M \mapsto N$ é um R-**homomorfismo** ou **homomorfismo** de R-módulos se f preserva a adição e a lei de composição externa.

Um R-homomorfismo diz-se um R-**monomorfismo** ou um R-**epimorfismo** se for injetor ou sobrejetor, respectivamente.

É de verificação simples que $\ker(f)$ e $Im(f)$ são submódulos de M e N, respectivamente e, além disso, análogo aos morfismos de outras estrutras algébricas, é fácil ver que um R-homomorfismo $f : M \mapsto N$ é um R-epimorfismo se, e somente se, $Im(f) = N$ e que, f é um R-monomorfismo se, e somente se, $\ker(f) = \{0\}$.

Exemplo 3.1. Seja N um submódulo de um R-módulo M. Então a aplicação **inclusão**

$$\begin{aligned} i : N &\hookrightarrow M \\ x &\mapsto x \end{aligned}$$

é um R-homomorfismo. Em particular, a aplicação identidade de M, $1_M : M \mapsto M$ também é um R-homomorfismo.

Assim como para anéis, definimos o **módulo quociente** como sendo o conjunto

$$\frac{M}{N} = \{m + N : m \in M\},$$

onde M é um R-módulo e N um submódulo de M. E com isso, temos o teorema do homomorfismo para módulos.

Teorema 3.1. ***(Teorema do homomorfismo para módulos)*** *Sejam M e N dois R-módulos, $f : M \to N$ um R-homomorfismo, $j : M \to \dfrac{M}{\ker(f)}$ a projeção canônica ao quociente e $i : Im(f) \to N$ a inclusão. Então existe uma única aplicação*

$$f^* : \frac{M}{\ker(f)} \to Im(f)$$

tal que

(i) $f = i \circ f^* \circ j$;

(iii) f^* *é um* R*-isomorfismo.*

A relação entre as aplicações do enunciado pode ser visualizada no diagrama abaixo

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle j}\downarrow & & \uparrow{\scriptstyle i} \\ \dfrac{M}{\ker(f)} & \xrightarrow{f^*} & Im(f) \end{array}$$

Definição 3.3. Seja $\{M\}_{i\in I}$ uma família de R-módulos, onde I é um conjunto de índices. Uma família $(m_i)_{i\in I} \in M$ é dita uma **família quase nula** se $m_i = 0$, exceto para um número finito de índices.

A noção de soma direta que será apresentada a seguir é bem familiar, já que se assemelha à definição dada no caso dos subespaços vetoriais. Para caracterizar essa soma direta faremos uso da proposição a seguir.

Proposição 3.1. *Seja* $\{M_i\}_{i\in I}$ *uma família de submódulos de um* R*-módulo* M*. As seguintes afirmações são equivalentes:*

(i) Todo elemento $m \in M$ *se escreve de um único modo na forma* $m = \sum_{i\in I} m_i$*, onde* $m_i \in M_i$*, para todo* $i \in I$ *e a família* $(m_i)_{i\in I}$ *é quase nula.*

(ii) $M = \sum_{i\in I} M_i$ *e, se* $\sum_{i\in I} m_i = 0$*, com* $m_i \in M_i$*, tem-se* $m_i = 0$*, para todo* $i \in I$*.*

(iii) $M = \sum_{i\in I} M_i$ *e* $M_j \bigcap \left(\sum_{i\neq j} M_i \right) = \{0\}$*, para todo* $j \in I$*.*

Um R-módulo M é dito **soma direta** de uma família $\{M_i\}_{i\in I}$ de submódulos se estiver verificada alguma (e portanto todas) das condições equivalentes da proposição anterior.

Para indicar que M é soma direta dos submódulos $\{M_i\}_{i\in I}$, usaremos o símbolo

$$M = \bigoplus_{i\in I} M_i,$$

e se $I = \{1, 2, \ldots, n\}$ escreveremos

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_n.$$

Um submódulo N de um R-módulo M é chamado um **somando direto** de M se existe um outro R-módulo N_0 tal que $M = N \oplus N_0$.

Exemplo 3.2. Considere o $\mathbb{Z}$-módulo $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. É de fácil verificação que $H_1 = \{\overline{0}, \overline{2}, \overline{4}\}$ e $H_2 = \{\overline{0}, \overline{3}\}$ são submódulos de $\mathbb{Z}_6$. E ainda,

$$H_1 \cap H_2 = \{\overline{0}\}$$

e

$$H_1 + H_2 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\} = \mathbb{Z}_6.$$

Logo, $\mathbb{Z}_6 = H_1 \bigoplus H_2$.

Dado um R anel, denotaremos por $R^{(I)}$ o conjunto de todas as famílias quase-nulas $(\lambda_i)_{i\in I}$, onde $\lambda_i \in R$, para todo $i \in I$.

Definição 3.4. Seja $\{x_i\}_{i\in I}$ uma família de elementos de um R-módulo M.

(i) Dizemos que um elemento $x \in M$ é uma **combinação linear** dos elementos da família se existe $(\lambda_i)_{i\in I} \in R^{(I)}$ tal que

$$x = \sum_{i\in I} \lambda_i x_i.$$

(ii) A família $\{x_i\}_{i\in I}$ é **linearmente independente** ou **livre** se para toda $(\lambda_i)_{i\in I} \in R^{(I)}$ tem-se

$$x = \sum_{i\in I} \lambda_i x_i = 0 \implies \lambda_i = 0, \text{ para todo } i \in I.$$

(iii) A família $\{x_i\}_{i\in I}$ é uma **base** de M se é uma família livre e gera todo M.

(iv) Um R-módulo M é chamado **livre** se tem uma base.

Se $\{x_i\}_{i\in I}$ é uma base de um R-módulo M então

$$M = \bigoplus_{i\in I} Rx_i.$$

Consequentemente, um conjunto S de elementos de um R-módulo M é uma base se, e somente se, todo elemento $m \in M$ pode ser escrito de maneira única como combinação linear finita dos elementos de S.

3.1.1 Módulos semissimples

Um R-módulo M é chamado **semissimples** se todo submódulo de M é um somando direto. Equivalentemente, M é semissimples se, e somente se, M é uma soma direta de submódulos simples. Um anel R é chamado **semissimples** se o módulo ${}_RR$ é semissimples.

Exemplo 3.3. (a) Se $\mathbb{K}$ é um corpo, todo $\mathbb{K}$-espaço vetorial é um $\mathbb{K}$-módulo semissimples.

(b) Todo módulo simples é semissimples.

Teorema 3.2. *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.

Agora, iremos descrever a estrutura dos anéis semissimples, começando de informações sobre seus ideais bilaterais. Nosso objetivo é caracterizar os anéis simples que são somandos diretos na decomposição de um anel semissimples.

Dada uma decomposição de um anel semissimples R como uma soma direta de ideais minimais à esquerda, reordenando se necessário, podemos agrupar os ideais à esquerda isomorfos juntos.

$$R = L_{11} \oplus \cdots \oplus L_{1r_1} \oplus L_{21} \oplus \cdots \oplus L_{2r_2} \oplus \cdots \oplus L_{s1} \oplus \cdots \oplus L_{sr_s}$$

Com a notação acima, $L_{ij} \simeq L_{ik}$ e $L_{ij}L_{kh} = \{0\}$, se $i \neq k$. Ainda sabemos que todo ideal minimal à esquerda de R é isomorfo a um dos ideais na decomposição de R dada acima.

Teorema 3.3. *Com a notação acima, seja A_i a soma de todos ideais à esquerda isomorfos a $L_{i1}, 1 \leq i \leq s$. Então:*

(i) Cada A_i é um ideal bilateral minimal de R.

(ii) $A_iA_j = \{0\}$ se $i \neq j$.

(iii) $R = \bigoplus_{i=1}^{s} A_i$ como anel, onde s é o número de classes isomórficas de ideais à esquerda minimais de R.

Corolário 3.1. *Os ideais $A_i, 1 \leq i \leq s$, definidos acima são anéis simples, ou seja, seus únicos ideais bilaterais são os triviais.*

Proposição 3.2. *Seja $R = \bigoplus_{i=1}^{s} A_i$ a decomposição de um anel semissimples R como uma soma direta de ideais bilaterais minimais. Então*

(i) Todo ideal bilateral I de R pode ser escrito na forma $I = A_{i_1} \oplus \cdots \oplus A_{i_t}$, onde $1 \leq i_1 < \cdots < i_t \leq s$.

(ii) Se $R = \bigoplus_{j=1}^{r} B_j$ *é uma outra decomposição de* R *em soma direta de ideais minimais bilaterais, então* $r = s$ *e, após uma possível renumeração de índices,* $A_i = B_i$*, para todo* i*.*

Os únicos ideais bilaterais minimais de um anel semissimples R são chamados **componentes simples** de R. Os elementos $\{e_1, \ldots, e_t\}$ do teorema que enunciaremos a seguir são chamados de **idempotentes centrais primitivos** de R.

Teorema 3.4. *Se* $R = \bigoplus_{i=1}^{s} A_i$ *é uma decomposição de um anel semissimples como uma soma direta de ideais bilaterais minimais, então existe uma família* $\{e_1, \ldots, e_t\}$ *de elementos de* R *tais que:*

(i) e_i *é um idempotente central,* $1 \leq i \leq t$*.*

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

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

(iv) e_i *não pode ser escrito como* $e_i = e_i^{'} + e_i^{''}$ *onde* $e_i^{'}, e_i^{''}$ *são idempotentes centrais tais que* $e_i^{'}, e_i^{''} \neq 0$ *e* $e_i^{'} e_i^{''} = 0, 1 \leq i \leq t$*.*

Até o momento vimos que um anel semissimples pode ser escrito como a soma direta de componentes simples. Ainda que não seja nosso objetivo, neste trabalho aprofundarmos na teoria de módulos. O próximo passo é ver estes anéis simples da decomposição. Passando pela teoria de anéis com condições de cadeia (anéis neotherianos e artinianos) e por resultados como o da Densidade de Jacobson e o Lema de Schur conseguimos mostrar um dos mais importantes resultados da teoria que é o Teorema de Wedderburn-Artin. Iremos encerrar essa seção com o enunciado desse importante teorema que em resumo, nos dá a descrição das componentes simples na decomposição de um anel semissimples.

Teorema 3.5 (Teorema de Wedderbun-Artin)**.** *Um anel* R *é semissimples se, e somente se, ele é 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, essa decomposição é única a menos de uma possível permutação conveniente de índices e de isomorfismos dos anéis de divisão.

3.2 Ánéis de grupo

Sejam G um grupo e R um anel com unidade. Construiremos um R-módulo onde os elementos de G são uma base, e usaremos as operações de G e R para definir uma estrutura de anel sobre esse módulo.

Seja RG o conjunto de todas as combinações lineares da forma

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

em que $a_g \in R$ e $a_g = 0$, para quase todo $g \in G$, isto é, tem-se uma quantidade finita de coeficientes não nulos em cada soma. Dado $\alpha \in RG$, definimos o **suporte** de α, denotado por $\text{supp}(\alpha)$, como o subconjunto de elementos de G que efetivamente aparecem na expressão de α, ou seja,

$$\text{supp}(\alpha) = \{g \in G : a_g \neq 0\}.$$

É direto da definição que dados $\alpha, \beta \in RG$, temos que $\alpha = \beta$ se, e somente se, $a_g = b_g$, para todo $g \in G$.

Para dar a RG uma estrutura de anel, definimos a adição e a multiplicação como segue

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

$$\alpha \cdot \beta = \sum_{g \in G} a_g g \cdot \sum_{g \in G} b_g g = \sum_{g,h \in G} a_g b_h gh.$$

Reorganizando os termos, podemos reescrever a multiplicação como

$$\alpha \cdot \beta = \sum_{u \in G} d_u u,$$

onde

$$d_u = \sum_{gh=u} a_g b_h.$$

Desta forma, RG é um anel com as operações descritas acima. Mais do que isso, RG é um anel com unidade $1 = \sum_{g \in G} u_g g$, onde o coeficiente correspondente à unidade do grupo é igual a 1 e $u_g = 0$ para todos os outros elementos de G.

Também podemos definir em RG a multiplicação de elementos de RG por elementos λ de R da seguinte forma

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

Com as 3 operações definidas acima, é possível verificar que RG é um R-módulo e, ainda, que se R é um anel comutativo, RG é uma R-álgebra.

Definição 3.5. O conjunto RG, com as operações definidas acima, é chamado de **anel de grupo** de G sobre R. No caso em que R é comutativo, RG é chamado de **álgebra de grupo** de G sobre R.

Podemos definir uma aplicação $i : G \mapsto RG$, fixando para cada elemento $x \in G$, o elemento $i(x) = \sum_{g \in G} a_g g$, onde $a_x = 1$ e $a_g = 0$, se $g \neq x$. Desta forma podemos enxergar G como um subconjunto de RG e assim, podemos dizer que G é uma base de RG sobre R. Então, se G é um grupo finito, a dimensão de RG sobre R é precisamente $|G|$.

Se considerarmos a aplicação $\varphi : R \mapsto RG$ dada por $\varphi(r) = \sum_{g \in G} a_g g$, onde $a_{1_G} = r$ e $a_g = 0$, se $g \neq 1_G$, não é dificil ver que φ é um homomorfismo injetor de anéis, e assim, R pode ser visto como um subanel de RG.

Com as identificações acima, dados $r \in R$ e $g \in G$, temos que $rg = gr$ em RG e assim, se R for um anel comutativo, temos que $R \subset Z(RG)$ (R está contido no centro de RG).

Proposição 3.3. *Seja $f : G \mapsto H$ um homomorfismo de grupos. Existe um único homomorfismo de anéis $f^* : RG \mapsto RH$ tal que $f^*(g) = f(g)$, para todo $g \in G$. Se R é um anel comutativo, então f^* é um homomorfismo de R-álgebras. Além disso, se f é um epimorfismo (monomorfismo), então f^* é um epimorfismo (monomorfismo).*

Observe que se $H = \{1\}$, então a Proposição 3.3 mostra que a aplicação trivial $G \mapsto \{1\}$ induz a um homomorfismo de anéis $\epsilon : RG \mapsto R$ tal que

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

Definição 3.6. O homomorfismo ϵ anterior é chamado de **aplicação de aumento** de RG, e seu núcleo, denotado por $\Delta(G)$, é chamado de **ideal de aumento** de RG.

Note que se $\alpha = \sum_{g \in G} a_g g$ pertence a $\Delta(G)$, então

$$\epsilon(\alpha) = \epsilon\left(\sum_{g \in G} a_g g\right) = \sum_{g \in G} a_g = 0.$$

Logo, podemos reescrever α como

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

Note que todos os elementos da forma $g - 1$, com $g \in G$, pertencem a $\Delta(G)$. A observação acima mostra que $\{g - 1 : g \in G, g \neq 1\}$ é um conjunto de geradores de $\Delta(G)$ sobre R. Observe que esse conjunto é linearmente independente.

Proposição 3.4. *O conjunto $\{g - 1 : g \in G, g \neq 1\}$ é uma base de $\Delta(G)$ sobre R, isto é,*

$$\Delta(G) = \left\{ \sum_{g \in G} a_g (g - 1) : g \in G, g \neq 1, a_g \in R \right\}.$$

Particulamente, se R é um anel comutativo e G um grupo finito, então $\Delta(G)$ é um R-módulo livre de dimensão $|G| - 1$.

3.2.1 Ideais de aumento

Queremos encontrar condições sobre R e G de modo que possamos decompor o anel de grupo RG como uma soma direta de subanéis. Nosso principal interesse está em determinar em que condições RG é um anel semisimples e em poder escrevê-lo como uma soma direta de ideais minimais. Inicialmente estudaremos a relação entre subgrupos de G e ideais de RG. Dados um grupo G e um anel R, denotamos por $S(G)$ o conjunto de todos os subgrupos de G e por $I(RG)$ o conjunto de todos os ideais à esquerda de RG.

Seja $H \in S(G)$ um subgrupo. Denotamos por $\Delta_R(G,H)$ o ideal à esquerda de RG gerado por $\{h-1 : h \in H\}$, isto é,

$$\Delta_R(G,H) = \left\{ \sum_{h\in H} \alpha_h(h-1) : \alpha_h \in R \right\}.$$

Quando estivermos lidando com um anel R fixo, denotaremos simplesmente por $\Delta(G,H)$. Note que $\Delta(G,G) = \Delta(G)$.

Lema 3.1. *Seja H um subgrupo de um grupo G e seja S um conjunto de geradores de H. O conjunto $\{s-1 : s \in S\}$ é um conjunto de geradores de $\Delta(G,H)$ como um ideal à esquerda de RG.*

Temos da teoria de grupos que se H é um subgrupo de G, então para $x \in G$, o conjunto $xH = \{xh : \ h \in H\}$ é a classe lateral à esquerda de H em G. E essas classes definem uma partição em G. Para dar uma melhor descrição de $\Delta_R(G,H)$, denotaremos por $\tau = \{q_i\}_{i\in I}$ um conjunto completo de representantes de classes à esquerda de H em G. Escolhemos para representante da classe H em τ o elemento identidade de G. Assim, todo elemento $g \in G$ pode ser escrito de forma única como $g = q_i h_j$, onde $q_i \in \tau$ e $h_j \in H$.

Proposição 3.5. *O conjunto $B_H = \{q(h-1) : q \in \tau, h \in H, h \neq 1\}$ é uma base de $\Delta_R(G,H)$ sobre R.*

Demonstração: Primeiro mostraremos que este conjunto é linearmente independente sobre R. Suponha que temos uma combinação linear

$$\sum_{i,j} r_{ij} q_i (h_j - 1) = 0,$$

com $r_{ij} \in R$. Assim, podemos escrever

$$\sum_{i,j} r_{ij} q_i h_j = \sum_i \left(\sum_j r_{ij} \right) q_i.$$

Já que $h_j \neq 1$, para todo valor de j, segue que os membros da equação acima possuem suportes disjuntos. Como os elementos de G são linearmente independentes sobre R, segue que todos os coeficientes são iguais a 0. Particularmente, $r_{ij} = 0$, para todos i, j.

Para mostrar que B_H gera $\Delta_R(G,H)$, é suficiente mostrar que todo elemento da forma $g(h-1)$, com $g \in G$ e $h \in H$, pode ser escrito como uma combinação linear de elementos em B_H. Mas $g = q_i h_j$, para algum $q_i \in \tau$ e algum $h_j \in H$. Logo

$$g(h-1) = q_i h_j (h-1) = q_i(h_j h - 1) - q_i(h_j - 1)$$

e segue o resultado. ■

Se H é um subgrupo normal de G, então o homomorfismo canônico $\omega : G \mapsto G/H$ pode ser estendido ao epimorfismo $\omega^* : RG \mapsto R(G/H)$ tal que

$$\omega^*(\alpha) = \omega^* \left(\sum_{g \in G} a(g) g \right) = \sum_{g \in G} a(g)\omega(g).$$

Proposição 3.6. *Com a notação acima,* $\ker(\omega^*) = \Delta(G,H)$.

Corolário 3.2. *Seja H um subgrupo normal de um grupo G. Então $\Delta(G,H)$ é um ideal bilateral de RG e*

$$\frac{RG}{\Delta(G,H)} \simeq R(G/H).$$

Logo, $\Delta(G)$ é núcleo do epimorfismo ϵ induzido pela aplicação trivial $G \mapsto G/G = \{1\}$. Assim, podemos construir uma aplicação de $S(G)$ sobre $I(RG)$ tal que os subgrupos normais de G são levados em ideais bilaterais de RG.

Dado um ideal à esquerda $I \in I(RG)$, consideremos o conjunto

$$\nabla(I) = \{g \in G : g - 1 \in I\},$$

isto é,

$$\nabla(I) = G \cap (1 + I).$$

Afirmamos que $\nabla(I)$ é um subgrupo de G. De fato, se $g, h \in \nabla(I)$, então

$$gh - 1 = g(h-1) + g - 1 \in \nabla(I).$$

Logo, $gh \in \nabla(I)$. Também, se $g \in \nabla(I)$, então $g^{-1} - 1 = -g^{-1}(g-1) \in \nabla(I)$ e, portanto, $g^{-1} \in \nabla(I)$. Por fim, é possivel verificar que se I é um ideal bilateral de RG, então $\nabla(I)$ é um subgrupo normal em G.

Proposição 3.7. *Se $H \in S(G)$, então $\nabla(\Delta(G,H)) = H$.*

Essas aplicações não são inversas uma da outra. Dado um ideal $I \in I(RG)$, verifica-se que $\Delta(G, \nabla(I)) \subset I$, mas em geral, $\Delta(G, \nabla(I)) \neq I$. De fato, se $I = RG$, então $\nabla(RG) = \{g \in G : g - 1 \in RG\} = G$. Mas $\Delta(G, \nabla(RG)) = \Delta(G) \neq RG$.

3.2.2 Semissimplicidade

Agora, determinaremos condições suficientes e necessárias sobre R e G para que o anel de grupo RG seja semissimples. Antes, veremos alguns resultados sobre anuladores, conceito que nos será útil. Encerraremos a seção com a demonstração do Teorema de Maschke e com alguns corolários deste teorema, que são de suma importância no estudo dos anéis de grupo.

Definição 3.7. Seja X um subconjunto de um 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 à direita** de X como:

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

Dados um anel de grupo RG e um subconjunto finito X do grupo G, denotaremos por $\hat{X}$ o seguinte elemento de RG :

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

Lema 3.2. *Sejam H um subgrupo de G e R um anel. O $Ann_r(\Delta(G,H)) \neq \{0\}$ se, e somente se, H é finito. Neste caso, temos $Ann_r(\Delta(G,H)) = \hat{H} \cdot RG$. Além disso, se H é um subgrupo normal de G, então o elemento $\hat{H}$ é central em RG e temos*

$$Ann_r(\Delta(G,H)) = Ann_l(\Delta(G,H)) = RG \cdot H.$$

Demonstração: Suponha $Ann_r(\Delta(G,H)) \neq \{0\}$ e escolha $\alpha = \sum_{g \in G} a_g g \neq 0$ em $Ann_r(\Delta(G,H))$. Para cada elemento $h \in H$, temos $(h-1)\alpha = 0$. Portanto, $h\alpha = \alpha$, isto é ,

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

Tome $g_0 \in supp(\alpha)$. Logo $a_{g_0} \neq 0$ e assim a equação acima mostra que $hg_0 \in supp(\alpha)$, para todo $h \in H$. Já que $supp(\alpha)$ é finito, isso implica que H tem que ser finito.

Note que o argumento acima mostra que, sempre que $g_0 \in supp(\alpha)$, o coeficiente de todo elemento da forma hg_0 é igual ao coeficiente de g_0. Daí, podemos escrever α na forma

$$\alpha = a_{g_0}\hat{H}g_0 + a_{g1}\hat{H}g_1 + \cdots + a_{gt}\hat{H}g_t = \hat{H}\beta, \text{ com } \beta \in RG.$$

Isso mostra que se H é finito, então $Ann_r(\Delta(G,H)) \subset \hat{H} \cdot RG$. Já que $h\hat{H} = \hat{H}$ implica em $(h-1)\hat{H} = 0$, para todo $h \in G$. A inclusão oposta segue claramente.

Se H é um subgrupo normal de G, para qualquer $g \in G$, temos $g^{-1}Hg = H$. Portanto, $g^{-1}\hat{H}g = \sum_{x\in H} g^{-1}xg = \sum_{x\in H} x = \hat{H}$. Logo $\hat{H}g = g\hat{H}$, para todo $g \in G$, ou seja, $\hat{H}$ é central em G. Consequentemente $RG \cdot \hat{H} = \hat{H} \cdot RG$ e segue o resultado. ∎

Corolário 3.3. *Seja G um grupo finito. Então $Ann_l(\Delta(G)) = Ann_r(\Delta(G)) = R \cdot \hat{G}$.*

Lema 3.3. *Seja I um ideal bilateral de um anel R. Suponha que exista um ideal à esquerda J tal que $R = I \oplus J$ (como R-módulos à esquerda). Então $J \subset Ann_r(I)$.*

Demonstração: Considere $x \in J$ e $y \in I$. Como I é um ideal bilateral, J um ideal à esquerda e $R = I \oplus J$, temos

$$yx \in J \cap I = \{0\} \implies yx = 0 \implies x \in Ann_r(I).$$

∎

Lema 3.4. *Se o ideal de aumento $\Delta(G)$ é um somando direto de RG, como um RG-módulo, então G é finito e $|G|$ é invertível em R.*

Demonstração: Suponha que $\Delta(G)$ é um somando direto de RG. Daí pelo lema anterior temos $Ann_r(\Delta(G)) \neq 0$, já que sendo J ideal à esquerda tal que $R = \Delta(G) \oplus J$, então teremos $J \subset \Delta(G)$.

Como $RG = \Delta(G) \oplus J$ e $1 = e_1 + e_2$, onde $e_1 \in \Delta(G)$ e $e_2 \in J$, temos que

$$1 = \epsilon(e_1) + \epsilon(e_2).$$

Já que $e_2 = a\hat{G}$, para algum $a \in R$, temos que $a\epsilon(\hat{G}) = 1$; então, $a|G| = 1$. Isso mostra que $|G|^{-1} = a$, isto é, $|G|$ é invertível em R. ∎

Agora, vamos determinar condições necessárias e suficientes sobre R e G para que o anel de grupo RG seja semissimples.

Teorema 3.6 (Teorema de Maschke)**.** *Seja G um grupo. O anel de grupo RG é semissimples se, e somente se, valem as seguintes condições:*

(i) R é um anel semissimples.

(ii) G é um grupo finito.

(iii) $|G|$ é invertível em R.

Demonstração: Suponha que RG seja semissimples. Sabemos que $R \simeq RG/\Delta(G)$. Já que o quociente de um anel semisimples é semissimples, segue que R é semissimples. Como a semissimplicidade de RG implica que $\Delta(G)$ é um somando direto, o Lema 3.4 mostra que as condições (ii) e (iii) são verdadeiras.

Reciprocamente, suponha que as condições (i), (ii) e (iii) são verdadeiras e seja M um RG-submódulo de RG. Já que R é semissimples, segue que RG é semissimples como um R-módulo. Portanto, existe um R-módulo N de RG tal que $RG = M \oplus N$.

Seja $\pi : RG \mapsto M$ a projeção canônica associada à essa soma direta. Definimos a aplicação $\pi^* : RG \mapsto M$ por uma média

$$\pi^*(x) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gx), \text{ para cada } x \in RG.$$

Se provarmos que π^* é um RG-homomorfismo tal que $(\pi^*)^2 = \pi^*$ e $Im(\pi^*) = M$, então $\ker(\pi^*)$ é um RG-submódulo tal que $RG = M \oplus \ker(\pi^*)$ e o teorema está provado.

Já que π^* é um R-homomorfismo, para mostrar que ele é também um RG-homomorfismo, é suficiente mostrar que

$$\pi^*(ax) = a\pi^*(x), \text{ para todo } x \in G, \text{ para todo } a \in G.$$

Temos

$$\pi^*(ax) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gax) = \frac{a}{|G|} \sum_{g \in G} (ga)^{-1}\pi((ga)x).$$

Quando g percorre todos os elementos em G, o produto ga também percorre todos os elementos em G. Logo,

$$\pi^*(ax) = a\frac{1}{|G|} \sum_{t \in G} t^{-1}\pi(tx) = a\pi^*(x).$$

Já que π é uma projeção sobre M, sabemos que $\pi(m) = m$, para todo $m \in M$. Como M é um RG-módulo, temos $gm \in M$, para todo $g \in G$. Portanto,

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

Dado um elemento $x \in RG$, temos $\pi(gx) \in M$. Portanto, $\pi^*(x) \in M$ e daí $Im(\pi^*) \subset M$. Consequentemente $\pi^*(\pi^*(x)) = \pi^*(x)$, para todo $x \in RG$, ou seja, $(\pi^*)^2 = \pi^*$. O fato de $\pi^*(m) = m$, para todo $m \in M$, também mostra que $M \subset Im(\pi^*)$ e segue o teorema. ∎

O caso em que $R = \mathbb{K}$ é um corpo é de grande importância. Neste caso, $\mathbb{K}$ é sempre semissimples e $|G|$ é invertível em $\mathbb{K}$ se, e somente se, $|G| \neq 0$ em $\mathbb{K}$ e $car(\mathbb{K}) \nmid |G|$. Como na teoria de códigos estaremos lidando com corpos e grupos finitos, o corolário a seguir é fundamental.

Corolário 3.4. *Sejam G um grupo finito e $\mathbb{K}$ um corpo. Então $\mathbb{K}G$ é semissimples se, e somente se, $car(\mathbb{K}) \nmid |G|$.*

Veremos agora uma adaptação do Teorema de Wedderburn-Artin que nos dá muitas informações sobre a estrutura de álgebra de grupo.

Teorema 3.7. *Seja G um grupo finito e seja $\mathbb{K}$ um corpo tal que $car(\mathbb{K}) \nmid |G|$. Assim, temos que*

(i) *$\mathbb{K}G$ é uma soma direta de um número finito de ideais bilaterais $\{B_i\}_{1\leq i\leq r}$, os componentes simples de $\mathbb{K}G$. Cada B_i é um anel simples.*

(ii) *Qualquer ideal bilateral de $\mathbb{K}G$ é uma soma direta de alguns dos membros da família $\{B_i\}_{1\leq i\leq r}$.*

(iii) *Cada componente simples B_i é isomorfo a um anel de matrizes da forma $M_{n_i}(D_i)$, onde D_i é um anel de divisão contendo uma cópia de $\mathbb{K}$ em seu centro, e o isomorfismo*

$$\mathbb{K}G \overset{\phi}{\simeq} \bigoplus_{i=1}^{r} M_{n_i}(D_i)$$

é um isomorfismo de $\mathbb{K}$-álgebras.

(iv) *Em cada matriz $M_{n_i}(D_i)$, o conjunto*

$$I_i = \left\{ \begin{bmatrix} x_1 & 0 & \cdots & 0 \\ x_2 & 0 & \cdots & 0 \\ & & \cdots & \\ x_{n_i} & 0 & \cdots & 0 \end{bmatrix} : x_1, x_2, \ldots, x_{n_i} \in D_i \right\} \simeq D_i^{n_i}$$

é um ideal minimal à esquerda.

Dado $x \in \mathbb{K}G$, consideramos $\phi(x) = (\alpha_1, \ldots, \alpha_r) \in \bigoplus_{i=1}^{r} M_{n_i}(D_i)$ e definimos o produto de x por um elemento $m_i \in I_i$ por $xm_i = \alpha_i m_i$. Com esta definição I_i torna-se um KG-módulo simples.

(v) *$I_i \not\simeq I_j$, se $i \neq j$.*

(vi) *Qualquer KG-módulo simples é isomorfo a algum $I_i, 1 \leq i \leq r$.*

Corolário 3.5. *Seja G um grupo finito e seja $\mathbb{K}$ um corpo algebricamente fechado tal que $car(\mathbb{K}) \nmid |G|$. Então $\mathbb{K}G \simeq \bigoplus_{i=1}^{r} M_{n_i}(\mathbb{K})$ e $n_1^2 + n_2^2 + \cdots + n_r^2 = |G|$.*

Demonstração: Já que $car(\mathbb{K}) \nmid |G|$, temos pelo Teorema 3.7

$$\mathbb{K}G \simeq \bigoplus_{i=1}^{r} M_{n_i}(D_i),$$

onde D_i é um anel de divisão contendo uma cópia de $\mathbb{K}$ em seu centro.

Calculando as dimensões sobre $\mathbb{K}$ nos dois lados da equação acima, temos

$$|G| = \sum_{i=1}^{r} n_i^2 [D_i : \mathbb{K}],$$

e segue que cada anel de divisão é de dimensão finita sobre $\mathbb{K}$. Como $\mathbb{K}$ é algebricamente fechado, temos $D_i = \mathbb{K}, 1 \leq i \leq r$, e o resultado está provado. ∎

3.2.3 Álgebras de grupos abelianos

Apresentamos nesta seção uma descrição completa de um anel de grupo para um grupo abeliano finito sobre um corpo $\mathbb{K}$ tal que $car(\mathbb{K}) \nmid |G|$.

Primeiro, tratamos do caso em que G é cíclico. Assumimos $G = \langle a : a^n = 1 \rangle$ e $\mathbb{K}$ um corpo tal que $car(\mathbb{K}) \nmid |G|$. Considere a aplicação $\theta : \mathbb{K}[x] \mapsto \mathbb{K}G$ dada por

$$f(x) \in \mathbb{K}[x] \mapsto f(a) \in \mathbb{K}G,$$

onde $\mathbb{K}[x]$ é o anel de polinômios sobre $\mathbb{K}$ na indeterminada x. É fácil verificar que θ e um epimorfismo de anéis. Portanto, pelo teorema do homomorfismo de anéis,

$$\mathbb{K}G \simeq \frac{\mathbb{K}[x]}{ker(\theta)}, \text{ onde } ker(\theta) = \{f(x) \in \mathbb{K}[x] : f(a) = 0\}.$$

Já que $\mathbb{K}[x]$ é um domínio de ideais principais, $ker(\theta)$ é o ideal gerado por um polinômio $f_0(x)$, de menor grau, tal que $f_0(a) = 0$. É importante observar que, sob este isomorfismo, o elemento a é levado na classe $x + \overline{f_0} \in \dfrac{\mathbb{K}[x]}{\langle f_0(x) \rangle}$.

Como $a^n = 1$, temos $x^n - 1 \in ker(\theta)$. Note que se $f(x) = \sum_{i=0}^{r} k_i x^i$ é um polinômio de grau $r \leq n$, então temos $f(a) = \sum_{i=0}^{r} k_i a^i \neq 0$, pois os elementos $\{1, a, a^2, \ldots, a^{n-1}\}$ são linearmente independentes sobre $\mathbb{K}$. Logo $ker(\theta) = \langle x^n - 1 \rangle$ e

$$\mathbb{K}G \simeq \frac{\mathbb{K}[x]}{\langle x^n - 1 \rangle}.$$

Seja $x^n - 1 = f_1(x) f_2(x), \ldots, f_t(x)$ a decomposição de $x^n - 1$ como um produto de polinômios irredutíveis em $\mathbb{K}[x]$. Como assumimos $car(\mathbb{K}) \nmid n$, este polinômio é separável e assim, $f_i \neq f_j$ se $i \neq j$. Usando o Teorema Chinês do Resto, podemos escrever

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

Sob este isomorfismo, o gerador a é aplicado no elemento

$$\left(x + \overline{f_1(x)}, \ldots, x + \overline{f_t(x)}\right).$$

Se ξ_i denota uma raiz de $f_i(x), 1 \leq i \leq t$, então temos $\dfrac{\mathbb{K}[x]}{\langle f_i(x)\rangle} \simeq \mathbb{K}(\xi_i)$. Consequentemente,

$$\mathbb{K}G \simeq \mathbb{K}(\xi_1) \oplus \mathbb{K}(\xi_2) \oplus \cdots \oplus \mathbb{K}(\xi_t).$$

Como todos os elementos $\xi_i, 1 \leq i \leq t$ são raízes de $x^n - 1$, devemos mostrar que $\mathbb{K}G$ é isomorfo a uma soma direta de extensões ciclotômicas de $\mathbb{K}$. Sob este isomorfismo, o elemento a é levado no elemento $(\xi_1, \xi_2, \ldots, \xi_t)$.

Agora veremos uma descrição de $\mathbb{K}G$ para o caso de um grupo abeliano qualquer. Primeiro vamos calcular todos os somandos diretos da decomposição de $\mathbb{K}G$.

Lembramos que, para um dado inteiro d, o **polinômio ciclotômico** de ordem d, denotado por Φ_d, é o produto $\Phi_d = \prod_j (x - \xi_j)$, onde ξ_j percorre todas as d-ésimas raízes primitivas da unidade. Também sabemos que $x^n - 1 = \prod_{d|n} \Phi_d$, o produto de todos os polinômios ciclotômicos Φ_d em $\mathbb{K}[x]$, onde d é um divisor de n. Para cada d, seja $\Phi_d = \prod_{i=1}^{a_d} f_{d_i}(x)$ a decomposição de Φ_d como um produto de polinômios irredutíveis em $\mathbb{K}[x]$.

Logo a decomposição de $\mathbb{K}G$ pode ser escrita na forma

$$\mathbb{K}G \simeq \bigoplus_{d|n} \bigoplus_{i=1}^{a_d} \frac{\mathbb{K}[x]}{\langle f_{d_i}(x)\rangle} \simeq \bigoplus_{d|n} \bigoplus_{i=1}^{a_d} \mathbb{K}(\xi_{d_i}),$$

onde ξ_{d_i} denota uma raiz de $f_{d_i}(x), 1 \leq i \leq a_d$. Para um d fixo, todos os elementos ξ_{d_i} são raízes n-ésimas primitivas da unidade. Portanto, todos os corpos da forma $\mathbb{K}(\xi_{d_i}), 1 \leq i \leq a_d$, são iguais uns aos outros e podemos sempre escrever

$$\mathbb{K}G \simeq \bigoplus_{d|n} a_d \mathbb{K}(\xi_d),$$

onde ξ_d é uma raiz primitiva de ordem d e $a_d\mathbb{K}(\xi_d)$ denota a soma direta de a_d corpos diferentes, todos eles isomorfos a $\mathbb{K}(\xi_d)$.

Já que o grau de $f_{d_i}(x)$ é igual ao grau de $[\mathbb{K}(\xi_d) : \mathbb{K}]$, os polinômios $f_{d_i}(x), 1 \leq i \leq a_d$, possuem o mesmo grau. Logo, tomando os graus na decomposição de Φ_d, temos

$$\phi(d) = a_d[\mathbb{K}(\xi_d) : \mathbb{K}],$$

onde ϕ denota a função de Euler, a saber

$$\phi(d) = |\{n \in \mathbb{Z} : 1 \leq n < d, mdc(n, d) = 1\}|.$$

Já que G é um grupo cíclico de ordem n, para cada divisor d de n, o número de elementos de ordem d em G, que denotamos por n_d, que é precisamente $\Phi(d)$. Portanto, podemos escrever

$$a_d = \frac{n_d}{[\mathbb{K}(\xi_d) : \mathbb{K}]}.$$

Teorema 3.8. *Sejam G um grupo abeliano finito de ordem n e $\mathbb{K}$ um corpo tal que $car(\mathbb{K}) \nmid n$. Então*

$$\mathbb{K}G \simeq \bigoplus_{d|n} a_d \mathbb{K}(\xi_d),$$

onde ξ_d denota uma raiz primitiva da unidade de ordem d e $a_d = \dfrac{n_d}{[\mathbb{K}(\xi_d) : \mathbb{K}]}$. Nesta fórmula, n_d denota o número de elementos de ordem d em G.

Corolário 3.6. *Seja G um grupo abeliano finito de ordem n e seja $\mathbb{K}$ um corpo tal que $car(\mathbb{K}) \nmid n$. Se $\mathbb{K}$ contém uma raiz primitiva da unidade de ordem n, então*

$$\mathbb{K}G \simeq \underbrace{\mathbb{K} \oplus \cdots \oplus \mathbb{K}}_{n}.$$

Se G e H são grupos isomorfos então é claro que os anéis de grupo RG e RH, sobre um anel qualquer R, também são isomorfas. Porém, a recíproca não é verdadeira. Vejamos agora um contra-exemplo para esta afirmação. Se G e H são grupos abelianos não isomorfos de mesma ordem n e $\mathbb{K}$ é um corpo tal que $car(\mathbb{K}) \nmid n$, que contém uma raiz primitiva da unidade de ordem n, então o corolário anterior mostra que

$$\mathbb{K}G \simeq \underbrace{\mathbb{K} \oplus \cdots \oplus \mathbb{K}}_{n} \simeq \mathbb{K}H.$$

Por exemplo, se C_2 e C_4 denotam os grupos cíclicos de ordem 2 e 4 respectivamente, então para as álgebras de grupo complexas temos

$$\mathbb{C}(C_2 \times C_2) \simeq C \oplus C \oplus C \oplus C \simeq \mathbb{C}C_4,$$

mas $C_2 \times C_2$ e C_4 não são isomorfos.

Este fato é o nosso primeiro contato com o conhecido **problema de isomorfismo**: "para quais condições sobre R e G o isomorfismo de anéis $RG \simeq RH$ implica que $G \simeq H$?" O problema do isomorfismo consiste em verificar se dois grupos serão isomorfos sempre que seus anéis de grupo o forem.

No próximo capítulo, iremos analisar os códigos corretores de erros quando realizados sobre as álgebras de grupo, para que assim possamos responder à seguinte pergunta: a que estrututra corresponde um código realizado sobre uma álgebra de grupo, em especial, para códigos cíclicos? Além disso, iremos dar ênfase sobre as vantagens que obtemos na realização de códigos sobre diferentes estruturas algébricas.

4 Códigos cíclicos sobre álgebras de grupo

Neste capítulo iremos utilizar o que foi desenvolvido nos capítulos 2 e 3 para apresentar uma visão dos códigos corretores de erros sobre álgebras de grupo, em especial apresentaremos como a teoria de códigos se desenvolve sobre álgebras de grupo sobre grupos cíclicos. O objetivo principal aqui é revisitar os resultados sobre códigos cíclicos, porém acrescentando às estruturas de espaço vetorial e anel a estrutura de álgebra de grupo. Iremos investigar as vantagens que obtemos ao realizar códigos cíclicos sobre essa estrutura algébrica e visualizar os resultados obtidos sobre anéis de polinômios agora sobre essa nova estrutura. O estudo de códigos no contexto das álgebras de grupo vem sendo estudado por diversos matemáticos e hoje já existe uma quantidade grande de trabalhos que servem de base para o início dos estudos sobre o tópico. Para mais detalhes do que iremos apresentar a seguir sugerimos (ALDERETE, 2018), (BERNAL; RÍO; SIMÓN, 2009) e (LUCHETTA, 2005).

4.1 Códigos de grupo

Um **código de grupo** (à esquerda) de comprimento n é um código linear que é imagem de um ideal (à esquerda) de uma álgebra de grupo via um isomorfismo

$$\mathbb{K}G \to \mathbb{K}^n$$

que aplica G na base canônica de $\mathbb{K}^n$.

Definição 4.1. Se G é um grupo de ordem n e $C \subset \mathbb{K}^n$ é um código linear então C é um G-**código** (à esquerda) se existe uma bijeção entre a base canônica de $\mathbb{K}^n$ e G que se estende a um isomorfismo $\mathbb{K}^n \to \mathbb{K}G$ que aplica C em um ideal (à esquerda) de $\mathbb{K}G$.

Assim, um código de grupo (à esquerda) é um código linear que é um G-código (à esquerda) para algum grupo G. De acordo com o tipo de grupo que estamos considerando, damos nomes mais específicos para estes códigos. Por exemplo, um **código de grupo cíclico** (ou abeliano, ou solúvel,...) é um código linear que é um G-código para algum grupo cíclico (ou abeliano, ou solúvel,...) G.

O estudo destes código de grupo tem obtido grande avanço nos últimos anos. E diversos autores têm se dedicado a obter resultados para diferentes tipos de grupo. Em (BERNAL; RÍO; SIMÓN, 2009), os autores trabalham com código de grupo para grupos que possuem uma certa decomposição em dois subgrupos abelianos. Em sua tese de doutorado, (ALDERETE, 2018), Alderete generaliza alguns dos resultados de Bernal, del

Río e Símon para o caso de grupos que se decompõem em mais subgrupos abelianos. Neste trabalho, nosso foco é apresentar uma parte do que já se existe na literatura sobre códigos de grupo sobre grupos cíclicos. Portanto, dedicaremos o resto deste capítulo para tratar especificamente deste caso. No que segue, apesar da definição formal acima de código de grupo cíclico, iremos nos referir aos códigos sobre álgebras de grupo, onde o grupo é cíclico, apenas como códigos cíclicos, pois queremos deixar mais evidente o paralelo que faremos com os já definidos códigos cíclicos no Capítulo 2. E dessa forma, procuramos deixar clara a quantidade de ferramentas que podemos ganhar utilizando diferentes estruturas algébricas nestes códigos.

4.2 Códigos sobre álgebras de grupo cíclico

Sejam $\mathbb{K}$ um corpo e $G = \{1, a, \ldots, a^{n-1}\}$ um grupo cíclico de ordem n tal que $car(\mathbb{K})$ não divide n. Note que a álgebra de grupo $\mathbb{K}G$ de G sobre $\mathbb{K}$ é um $\mathbb{K}$-espaço vetorial de dimensão n e, portanto, isomorfo a $\mathbb{K}^n$. Consideramos o seguinte isomorfismo linear:

$$\begin{aligned} \psi : \mathbb{K}^n &\rightarrow \mathbb{K}G \\ (c_0, c_1, \ldots, c_{n-1}) &\mapsto c_0 + c_1 a + \cdots + c_{n-1}a^{n-1}. \end{aligned}$$

Desta forma, cada palavra de um código C em $\mathbb{K}^n$ pode ser vista como um elemento de $\mathbb{K}G$ ou vice-versa. E ainda, observe que se $c = (c_0, c_1, \ldots, c_{n-1})$ é uma palavra de um código C, então o peso de C é $\omega(c) = |\text{supp}(\psi(c))|$. Considere agora o epimorfismo de anéis dado por

$$\begin{aligned} \theta : \mathbb{K}[x] &\rightarrow \mathbb{K}G \\ f(x) &\mapsto f(a). \end{aligned}$$

Pelo Teorema do homomorfismo de anéis temos que

$$\mathbb{K}G \simeq \frac{\mathbb{K}[x]}{ker\theta}.$$

Na Subseção 3.2.3 já apresentamos o resultado a seguir para o caso mais geral de G ser um grupo abeliano. No entanto, a seguir vamos mostrar com mais detalhes o mesmo resultado para o caso de G de ser cíclico.

Proposição 4.1. $ker\theta = \langle x^n - 1 \rangle$.

Demonstração: Note que dado $q(x) \in \langle x^n - 1 \rangle$, temos que $q(x) = f(x) \cdot (x^n - 1)$, onde $f(x) \in \mathbb{K}[x]$. Daí, $\theta(q(x)) = q(a) = f(a) \cdot (a^n - 1) = f(a) \cdot 0 = 0$. Logo, $\langle x^n - 1 \rangle \subset \ker \theta$.

Por outro lado, seja $f(x) \in \ker\theta$. Pelo algoritmo da divisão, existem $q(x), r(x) \in \mathbb{K}[x]$ tais que

$$f(x) = q(x) \cdot (x^n - 1) + r(x),$$

com $r(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$. Daí temos que

$$f(a) = q(a) \cdot (a^n - 1) + r(a),$$

e como $f(x) \in \ker\theta$ e $a^n - 1 = 0$, segue que $r(a) = 0$. Assim,

$$r(a) = 0 \implies b_0 + b_1a + \cdots + b_{n-1}a^{n-1} = 0,$$

e $\{1, a, \ldots, a^{n-1}\}$ é base de $\mathbb{K}G$, o que mostra que $r(x) = 0$ e, assim, $f(x) = q(x) \cdot (x^n - 1)$, isto é, $f(x) \in \langle x^n - 1\rangle$. ∎

Com isso, temos que além de isomorfos como espaços vetoriais,

$$\mathbb{K}G \simeq \frac{\mathbb{K}[x]}{ker\theta} = \frac{\mathbb{K}[x]}{\langle x^n - 1\rangle} = R_n$$

como anéis.

Proposição 4.2. *Seja $G = \langle a\rangle$ um grupo cíclico de ordem n gerado por a. Todo ideal de $\mathbb{K}G$ é da forma $\mathbb{K}Gf(a)$, onde f(x) é um divisor de $x^n - 1$.*

Demonstração: Recorde que os ideais de R_n são gerados por $f(x) \in \mathbb{K}[x]$, onde $f(x)$ é um divisor de $x^n - 1$, e como $\mathbb{K}G$ é isomorfo a R_n, o resultado segue. ∎

Assim, concluímos que um código $C \subset \mathbb{K}^n$ é cíclico se, e somente se, $\psi(C)$ é da forma $\psi(C) = \mathbb{K}Gf(a)$, onde $f(x) \in \mathbb{K}[x]$ é um divisor de $x^n - 1$. Por essa razão será comum chamarmos $\psi(C)$ de código cíclico quando na verdade o código cíclico que estaremos nos referindo será o subespaço vetorial C de $\mathbb{K}^n$.

Assim como assumimos anteriormente, o polinômio $g(x)$ denotará um divisor de $x^n - 1$ e denotaremos por $h(x)$ o quociente

$$h(x) = \frac{x^n - 1}{g(x)}.$$

Definição 4.2. Seja $\psi(C) = \mathbb{K}Gg(a)$ um código cíclico. Denominamos $g(a)$ de **gerador principal** de C.

Podemos ter vários geradores para $\psi(C)$, mas estamos interessados no que é proveniente da fatoração de $x^n - 1$. Seja $\alpha \in C$, onde, por abuso de notação, $C = \langle g(a)\rangle$ é um código cíclico. Então $\alpha = k(a) \cdot g(a)$ para algum $k(a) \in \mathbb{K}G$, onde $g(x) \in \mathbb{K}[x]$ é um divisor de $x^n - 1$.

Quando $\alpha = k(a) \cdot g(a) \in C$ utilizaremos um abuso de notação e escreveremos o correspondente em R_n por $\alpha(x) = k(x) \cdot g(x)$.

Proposição 4.3. *Um elemento $f(a)$ pertence a $\mathbb{K}Gg(a)$ se, e somente se, $f(a)h(a) = 0$ em $\mathbb{K}G$.*

Demonstração: Seja $f(a) \in \mathbb{K}Gg(a)$. Assim, $f(a) = \delta(a) \cdot g(a)$, com $\delta(a) \in \mathbb{K}G$. Logo, $f(a)h(a) = \delta(a) \cdot g(a) \cdot h(a)$, isto é, $f(a) \cdot h(a) = \delta(a) \cdot (a^n - 1) = 0$.

Por outro lado, suponha que $f(a) \cdot h(a) = 0$ em $\mathbb{K}G$. Como $g(x)$ e $h(x)$ são relativamente primos, existem $r(x), s(x) \in \mathbb{K}[x]$ de maneira que

$$r(x) \cdot g(x) + s(x)h(x) = 1.$$

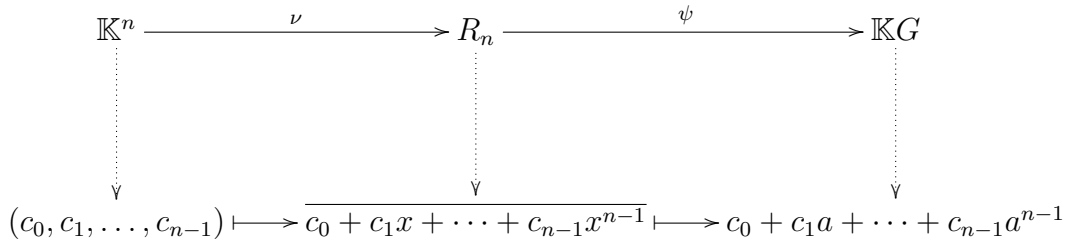
Desta forma,

$$r(a)g(a) + s(a)h(a) = 1 \implies f(a)r(a)g(a) + f(a)s(a)h(a) = f(a).$$

Como G é um grupo cíclico, $\mathbb{K}$ é um corpo e, por hipótese, $f(a) \cdot h(a) = 0$, então $f(a)s(a)h(a) = f(a)h(a)s(a) = 0$ e, portanto, $f(a) \in \mathbb{K}G$. ∎

O elemento $h(a)$ recebe o nome de **elemento de teste** do código $C = \langle g(a) \rangle$.

O diagrama a seguir nos dá uma boa noção da importância de analisar os códigos cíclicos sobre diferentes estruturas algébricas.



Em $\mathbb{K}^n$, temos que os códigos cíclicos são subespaços vetoriais gerados a partir de matrizes. Em R_n, são ideais gerados por um polinômio divisor de $x^n - 1$, o que nos dá uma vantagem de custo do ponto de vista computacional. Por fim, em $\mathbb{K}G$ temos que os códigos cíclicos também são ideais, só que dessa vez gerados por elementos da própria álgebra de grupo.

4.3 Matrizes geradora e teste de paridade

Vamos agora usar o que já sabemos sobre códigos cíclicos em $\mathbb{K}^n$ para determinar matrizes geradoras e teste de paridade em $\mathbb{K}G$, mediante o isomorfismo que há entre $\mathbb{K}^n$ e $\mathbb{K}G$.

Teorema 4.1. *Seja $I = \mathbb{K}Gg(a)$, onde $g(x) = g_0 + g_1x + \cdots + g_sx^s$ é um divisor de $x^n - 1$ de grau s. Então $\mathcal{B} = \{g(a), ag(a), \ldots, a^{n-s-1}g(a)\}$ é uma base de I como espaço vetorial*

sobre $\mathbb{K}$*, a dimensão de* I *é* $n-s$ *e o código* $C=\psi^{-1}(I)$ *tem matriz geradora dada por*

$$G=\begin{pmatrix} g_0 & g_1 & \dots & g_s & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_s & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \dots & 0 & \dots & g_0 & \dots & g_s \end{pmatrix}.$$

Demonstração: O resultado segue direto do Teorema 2.4 e do isomorfismo entre R_n e $\mathbb{K}G$. ∎

Lembre-se que dada uma matriz geradora do código C, basta multiplicar uma palavra do código da fonte pela matriz para obter uma codificação, isto é, um código de canal.

Exemplo 4.1. Considere o alfabeto $\mathbb{F}_2$ e $G=\{1,a,a^2,a^3,a^4,a^5,a^6,a^7,a^8\}$ um grupo cíclico de ordem 9. Seja C o código com gerador principal dado por $g(a)=a^7+a^6+a^4+a^3+a+1$. Pelo Teorema 4.1, uma base para C é dada por

$$\mathcal{B}=\{a^7+a^6+a^4+a^3+a+1, a^8+a^7+a^5+a^4+a^2+a\}.$$

Como a dimensão de C é 2, então uma matriz geradora para ele é dada por

$$M=\begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Relembre de (2.1), que dado um polinômio $p(x)=p_0+p_1x+\cdots+p_tx^t$, chamamos de polinômio recíproco de $p(x)$, o polinômio $p^*(x)=x^tf(x^{-1})=p_t+p_{t-1}x+\cdots+p_0x^t$.

Proposição 4.4. *Sejam* $\mathbb{K}$ *um corpo,* $f(x),g(x)\in\mathbb{K}[x]$ *com* $f(x)$ *de grau* n *e considere os polinômios recíprocos* $f^*(x)$ *e* $g^*(x)$*. Se* $g(x)$ *divide* $f(x)$*, então* $g^*(x)$ *divide* $f^*(x)$*. Além disso, se* $g(x)$ *divide* x^n-1*, então* $g^*(x)$ *também divide* x^n-1*.*

Demonstração: Suponha que $g(x)$ divide $f(x)$. Daí, $f(x)=p(x)g(x)$, com $p(x)\in\mathbb{K}[x]$. É claro que o grau de $g(x)$ é menor ou igual ao grau de $f(x)$. Suponha então que o grau de $g(x)$ seja estritamente menor que o grau de $f(x)$, isto é, $gr(g(x))=m<n$. Desta forma,

$$\begin{aligned} f^*(x)=x^nf(x^{-1}) &= x^n[p(x^{-1})g(x^{-1})] \\ &= x^{n-m}p(x^{-1})x^mg(x^{-1}) \\ &= x^{n-m}p(x^{-1})g^*(x) \\ &= p^*(x)g^*(x), \end{aligned}$$

logo, $g^*(x)$ divide $f^*(x)$. Por outro lado, seja $q(x)=x^n-1$. Observe que

$$q^*(x)=x^n(x^{-n}-1)=1-x^n=-(x^n-1) \implies -q^*(x)=x^n-1.$$

Agora, note que acabamos de mostrar que se $g(x)$ divide x^n-1, então $g^*(x)$ divide $q^*(x)$, isto é, $g^*(x)$ divide $-(x^n-1)$ e, portanto, divide x^n-1. ∎

Lema 4.1. *Sejam $b = (b_0, \ldots, b_{n-1})$ e $c = (c_0, \ldots, c_{n-1})$. Então $\psi(b)\psi(c) = 0$ em $\mathbb{K}G$ se, e somente se, $b^* = (b_{n-1}, \ldots, b_0)$ é ortogonal ao vetor c e a toda troca cíclica deste vetor em $\mathbb{K}^n$.*

Demonstração: Note que $\psi(b) = \sum_{i=0}^{n-1} b_i a^i$ e $\psi(c) = \sum_{j=0}^{n-1} c_j a^j$. Daí,

$$\psi(b)\psi(c) = \sum_{i,j} (b_i c_j)(a^i a^j).$$

Assim,

$$\psi(b)\psi(c) = \sum_{k=0}^{n-1} d_k a^k,$$

com $d_k = \sum_{i+j=k \pmod n} b_i c_j$.

Desta forma, $\psi(b)\psi(c) = 0$ se, somente se, $d_k = 0$, isto é,

$$\begin{aligned}
b_{n-1}c_1 + b_{n-2}c_2 + b_{n-3}c_3 + \cdots + b_0 c_0 &= 0 \\
b_{n-1}c_2 + b_{n-2}c_3 + b_{n-3}c_4 + \cdots + b_0 c_1 &= 0 \\
b_{n-1}c_3 + b_{n-2}c_4 + b_{n-3}c_5 + \cdots + b_0 c_2 &= 0 \\
\cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots &= 0 \\
b_{n-1}c_0 + b_{n-2}c_1 + b_{n-3}c_2 + \cdots + b_0 c_{n-1} &= 0
\end{aligned}$$

Assim,

$$\begin{aligned}
(b_{n-1}, b_{n-2}, b_{n-3}, \ldots b_0) \cdot (c_1, c_2, c_3, \ldots, c_0) = b^* \cdot \sigma^{n-1}(c) &= 0 \\
(b_{n-1}, b_{n-2}, b_{n-3}, \ldots b_0) \cdot (c_2, c_3, c_4, \ldots, c_1) = b^* \cdot \sigma^{n-2}(c) &= 0 \\
(b_{n-1}, b_{n-2}, b_{n-3}, \ldots b_0) \cdot (c_3, c_4, c_5, \ldots, c_2) = b^* \cdot \sigma^{n-3}(c) &= 0 \\
\cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots &= 0 \\
(b_{n-1}, b_{n-2}, b_{n-3}, \ldots b_0) \cdot (c_0, c_1, c_2, \ldots, c_{n-1}) = b^* \cdot c &= 0
\end{aligned}$$

Como queríamos demonstrar. ∎

Teorema 4.2. *Seja C um código cíclico, onde $I = \psi(C) = \langle g(a) \rangle$, com $g(x)$ um divisor de $x^n - 1$ de grau s e M matriz geradora de C. Se $x^n - 1 = g(x)h(x)$, com $h(x) = h_0 + h_1 x + \cdots + h_{n-s}x^{n-s}$ então uma matriz teste de paridade de C é dada por*

$$H = \begin{pmatrix}
h_{n-s} & h_{n-s-1} & \ldots & \ldots & h_0 & 0 & \ldots & 0 \\
0 & h_{n-s} & \ldots & \ldots & h_1 & h_0 & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & h_{n-s} & h_{n-s-1} & h_{n-s-2} & \ldots & h_0
\end{pmatrix}$$

Demonstração: Note que cada entrada em HM é dada pela multiplicação de $(h_{n-1}, h_{n-2}, \ldots, h_0)$ por uma troca cíclica do vetor $(g_0, g_1, \ldots, g_{n-1})$. Pelo lema anterior e usando o fato de que $h(a)g(a) = 0$ em $\mathbb{K}G$, temos que $HM = 0$. ∎

Considere $\alpha \in \mathbb{K}G$, onde $\alpha = \sum_{i=0}^{m} \alpha_i a^{-i}$, onde $m \leq n-1$. Definimos o **elemento recíproco** de α por

$$\alpha^* = a^m \sum_{i=0}^{m} \alpha_i a^{-i} = a^m f\left(\frac{1}{a}\right).$$

Note que $\alpha^* \in \mathbb{K}G$.

Corolário 4.1. *Seja C um código cíclico, onde $I = \psi(C) = \langle g(a) \rangle$, com $g(x)$ um divisor de $x^n - 1$ de grau s. Então $C^\perp$ é cíclico e $C^\perp = \psi^{-1}(J)$, onde $J = \langle h^*(a) \rangle$.*

Demonstração: A demonstração é a análoga a apresentada no Teorema 2.5. ∎

Exemplo 4.2. Seja C um código cíclico com gerador principal $g(a) = 1 + a + a^2 \in \mathbb{F}_2 G$, com $G = \langle a \rangle$ um grupo finito de ordem 9. Fazendo $h(x) = \dfrac{x^n - 1}{g(x)}$ obtemos $h(x) = x^7 + x^6 + x^4 + x^3 + x + 1$. Daí, uma matriz teste de paridade do código C é

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

4.4 Zeros do Código Cíclico

A caracterização que vimos dos códigos cíclicos foi através de polinômios divisores de $x^n - 1$. Outra caracterização destes códigos é feita através das raízes do polinômio $x^n - 1$ e a descrevemos a seguir.

Sejam $x^n - 1 = \prod_i m_i(x)$ a fatoração de $x^n - 1$ em fatores mônicos irredutíveis sobre $\mathbb{K}$ e ξ uma raiz de $m_i(x)$ em alguma extensão de $\mathbb{K}$. Então $m_i(x)$ é o polinômio minimal de ξ sobre $\mathbb{K}$.

Consideremos o código cíclico C gerado por $m_i(x)$. Dado $f(x) \in \mathbb{K}[x]$, vimos que $f(a) \in C$ se, e somente se, $f(a) = k(a)m_i(a)$, para algum $k(a) \in \mathbb{K}G$, isto é, se, e somente se, $f(x) = k(x)m_i(x)$ e, neste caso, $f(\xi) = k(\xi)m_i(\xi) = 0$. Reciprocamente, se $f(\xi) = 0$, então $m_i(x) \mid f(x)$ e daí $f(a) \in C$. Enfim, $f(a) \in C$ se, e somente se, $f(\xi) = 0$. Temos assim o seguinte teorema:

Teorema 4.3. *Sejam $g(x)$ um divisor de $x^n - 1$ e $\xi_1, \xi_2, \ldots, \xi_u$ o conjunto das raízes de $g(x)$ num corpo de decomposição de $x^n - 1$ sobre $\mathbb{K}$. Então*

$$\psi(C) = \langle g(a) \rangle = \{f(a) \in \mathbb{K}G : f(x) \in \mathbb{K}[x], f(\xi_1) = 0, \ldots, f(\xi_u) = 0\}.$$

Observação 4.1. *Se $\{\xi_1, \xi_2, \ldots, \xi_u\}$ é qualquer conjunto de raízes de $x^n - 1$, então o polinômio gerador do código cíclico $\{f(a) \in \mathbb{K}G : f(x) \in K[x], f(\xi_1) = 0, \ldots, f(\xi_u) = 0\}$ é o mínimo múltiplo comum dos polinômios minimais para as raízes $\xi_1, \xi_2, \ldots, \xi_u$.*

Se $\mathbb{F}_q$ é um corpo finito com q elementos, dizemos que um elemento $\gamma \in \mathbb{F}_q$ é um **elemento primitivo** se a ordem de γ é $q-1$, isto é, $\gamma^{q-1} = 1$.

Vamos considerar $\{\xi_1, \xi_2, \ldots, \xi_u\}$ um conjunto de raízes de $x^n - 1$ num corpo de decomposição $\mathbb{F}$ do polinômio $x^n - 1$ e seja $[\mathbb{F} : \mathbb{K}] = d$ o grau da extensão $\mathbb{F}$ sobre $\mathbb{K}$ e C um código gerado por $g(a)$, onde $g(x) = (x - \xi_1) \ldots (x - \xi_u)$.

Dado $f(x) = \sum_{j=0}^{n-1} b_j x^j \in \mathbb{K}[x]$, pelo Teorema 4.3, $f(a) \in C$ se, e somente se, $f(\xi_i) = \sum_{j=0}^{n-1} b_j \xi_i^j = 0$, para $i = 1, \ldots, u$. Assim, nossa descrição do código C em $\mathbb{K}^n$ é:

$$C = \{(b_0, b_1, \cdots, b_{n-1}) \in \mathbb{K}^n : \ b_0 + b_1\xi_i + \cdots + b_{n-1}\xi_i^{n-1} = 0, \ \forall\, i = 1, \ldots, u\},$$

o que equivale ao conjunto dos elementos $b = (b_0, \ldots, b_{n-1}) \in \mathbb{K}^n$, tais que:

$$\underbrace{\begin{pmatrix} \xi_1^0 & \xi_1^1 & \xi_1^2 & \cdots & \xi_1^{n-1} \\ \xi_2^0 & \xi_2^1 & \xi_2^2 & \cdots & \xi_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \xi_u^0 & \xi_u^1 & \xi_u^2 & \cdots & \xi_u^{n-1} \end{pmatrix}}_{H_1} \cdot \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Note que H_1 possui entradas em $\mathbb{F}$ e além disso, se $b \in \mathbb{K}^n$ então

$$b \in C \quad \Leftrightarrow \quad H_1 b = 0.$$

Como $\mathbb{F}$ é uma extensão de $\mathbb{K}$, podemos ver $\mathbb{F}$ como espaço vetorial sobre $\mathbb{K}$ de dimensão finita d. E uma base de $\mathbb{F}$ é dada por $\mathcal{B} = \{1, \gamma, \ldots, \gamma^{d-1}\}$, onde γ é um elemento primitivo em $\mathbb{K}$ sobre $\mathbb{F}$. Então cada elemento $\xi_j^i \in \mathbb{F}$ pode ser escrito como combinação linear dos elementos de $\mathcal{B}$. Isto é,

$$\xi_j^i = \sum_{k=0}^{d-1} \lambda_k^{i,j} \gamma^k,$$

onde $\lambda_k^{i,j} \in \mathbb{K}$, com $i = 0, \ldots, n-1$ e $j = 1, \ldots, u$.

Representamos por $[\xi_j^i]$ o vetor coluna de $\mathbb{K}^d$ das coordenadas de ξ_j^i com relação à base $\mathcal{B}$. Então definimos

$$H_2 = \begin{pmatrix} [\xi_1^0] & [\xi_1^1] & [\xi_1^2] & \cdots & [\xi_1^{n-1}] \\ [\xi_2^0] & [\xi_2^1] & [\xi_2^2] & \cdots & [\xi_2^{n-1}] \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ [\xi_u^0] & [\xi_u^1] & [\xi_u^2] & \cdots & [\xi_u^{n-1}] \end{pmatrix}.$$

Assim, temos que

$$H_2 b = \begin{pmatrix} \lambda_0^{1,0} b_0 + \lambda_0^{1,1} b_1 + \lambda_0^{1,2} b_2 + \cdots + \lambda_0^{1,n-1} b_{n-1} \\ \vdots \\ \lambda_{d-1}^{1,0} b_0 + \lambda_{d-1}^{1,1} b_1 + \lambda_{d-1}^{1,2} b_2 + \cdots + \lambda_{d-1}^{1,n-1} b_{n-1} \\ \vdots \\ \lambda_0^{u,0} b_0 + \lambda_0^{u,1} b_1 + \lambda_0^{u,2} b_2 + \cdots + \lambda_0^{u,n-1} b_{n-1} \\ \vdots \\ \lambda_{d-1}^{u,0} b_0 + \lambda_{d-1}^{u,1} b_1 + \lambda_{d-1}^{u,2} b_2 + \cdots + \lambda_{d-1}^{u,n-1} b_{n-1} \end{pmatrix}$$

Proposição 4.5. *Dado $b \in \mathbb{K}^n$, $b \in C$ se, e somente se, $H_2 b = 0$, onde H_2 é a matriz anterior. Como as linhas de H_2 não são, necessariamente, linearmente independentes, escolhemos um conjunto maximal de linhas linearmente independentes e obtemos uma matriz H que ainda verifica*

$$b \in C \Leftrightarrow Hb = 0.$$

Como esta matriz é de posto máximo com esta propriedade, temos o seguinte:

Teorema 4.4. *A matriz H construída acima é uma matriz teste de paridade para C.*

Note que com essa última seção ganhamos mais opções para obtermos algoritmos de codificação e decodificação. E basicamente, o estudo matemático dos códigos sobre estruturas algébricas baseia-se nessa busca por melhores algoritmos. A utilização de diferentes estruturas algébricas, como foi possível perceber, nos retornam diferentes maneiras de manipular um mesmo código. O que nos dirá qual ou quais melhores ferramentas matemáticas utilizar são questões relacionadas ao custo de implementação desses algoritmos, especialmente computacionalmente. Ao falarmos em custo, também estamos nos referindo ao custo financeiro, mas não podemos deixar de lado o custo humano de preparação para utilizar tais algoritmos. Logo, a busca por métodos que também simplifiquem esses algoritmos obtidos é importante, já que os profissionais que cuidam de tal implementação, em geral, engenheiros, querem algo que funcione e seja confiável, mas que não sejam tão complexos para serem utilizados.

Considerações Finais

Neste trabalho, analisamos os códigos corretores de erros sobre diferentes estruturas algébricas e entendemos os benefícios que ganhamos ao fazer isso.

Inicialmente, estudamos os códigos sobre espaços vetoriais: os códigos lineares, que podem ser gerados a partir de matrizes. Vimos também que alguns códigos lineares são enxergados como ideais de um certo anel, e, ao fazê-los, estes códigos podem ser gerados a partir de polinômios, o que nos dá significativa vantagem na busca por códigos mais sofisticados, que afinal, é o que a teoria de códigos busca. Por fim, mas não menos importante, realizamos códigos sobre álgebras de grupo e percebemos que podemos gerá-los através de elementos da própria álgebra de grupo, facilitando ainda mais a busca por melhores códigos. Com esse breve estudo, já foi possível concluirmos que o estudo da teoria de códigos utilizando estruturas algébricas traz enormes avanços e essa mescla de teorias continua muito promissora, haja visto que constantemente novos resultados sobre estruturas algébricas são provados. A teoria de códigos corretores de erros está inserida no que chamamos de teoria da informação que está presente em praticamente todos os momentos da nossa vida. A transmissão de informação, especialmente por meios digitais, requer cada vez mais códigos seguros e bons. Isto é, com bons parâmetros e, de preferência, com baixo custo. Sendo assim, o desenvolvimento da teoria aqui apresentada será sempre objeto de estudos atuais e a utilização de novas ferramentas, como as estruturas algébricas, trará novas perspectivas para a área.

Do ponto de vista matemático, caminhos naturais na sequência deste trabalho seria estudar códigos de grupo sobre outros tipos de grupos, como por exemplo os abelianos, os solúveis, entre outros. No entanto, do ponto de vista da matemática aplicada ou até mesmo das engenharias, um outro caminho natural seria entender como funcionam os parâmetros dos códigos realizados sobre álgebras de grupo e daí avaliar o quão bons são estes códigos. O entendimento da qualidade dos códigos, especialmente para os engenheiros, tem uma razão óbvia: seria possível implementar estes códigos na prática? Neste trabalho não tínhamos essa ambição de responder tal pergunta, mesmo porque para a compreensão da implementação destes códigos necessitamos de um estudo mais aprofundado sobre conhecimentos de engenharia e transmissão de informação. Porém, vale ressaltar que o entendimento matemático da teoria nos dá, também, uma base para prosseguir os estudos nas áreas aplicadas da matemática.

Referências

ALDERETE, S. A. *Códigos corretores de erros sobre grupos com decomposição m - abeliana*. Tese (Doutorado) — UFBA/UFAL, Bahia, 2018. 54

BERNAL, J. J.; RÍO, Á. del; SIMÓN, J. J. An intrinsical description of group codes. *Designs, Codes and Cryptography*, Springer, v. 51, n. 3, p. 289–300, 2009. 54

GONÇALVES, A. *Introdução à álgebra*. 6. ed. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 2017. 12, 16, 17

HEFEZ, A.; FERNANDEZ, C. d. S. *Introdução à Álgebra Linear*. 2. ed. Rio de Janeiro: Coleção PROFMAT, SBM, 2016. 10

HEFEZ, A.; VILLELA, M. L. T. *Códigos corretores de erros*. Rio de Janeiro: Instituto de Matematica Pura e Aplicada, 2008. 12, 22

LUCHETTA, V. O. J. *Códigos cíclicos como ideais em álgebras de grupo*. Dissertação (Mestrado) — IME - USP, São Paulo, 2005. 54

MILIES, C. P.; SEHGAL, S. K. *An introduction to group rings*. Dordrecht: Kluwer Academic Publishers, 2002. 36