Trabalho apresentado no XXXVIII CNMAC, Campinas - SP, 2018.

**Proceeding Series of the Brazilian Society of Computational and Applied Mathematics**

# Códigos sobre Anéis de Grupos

João Antonio Camargo Neto[1]
Universidade Federal de Uberlândia, Uberlândia, MG
Alonso Sepúlveda Castellanos[2]
Faculdado de Matemática, UFU, Uberlândia, MG

**Definição:** Sejam RG um anel de grupo e $u \in RG$ não nulo, dizemos que u é um **divisor de zero à esquerda** de $RG$ se existe $v \in RG$, $v \neq 0$, tal que, $uv = 0$. De maneira análoga, $u$ é chamado **divisor de zero à direita** de $RG$ se $vu = 0$. Se $u$ é divisor de zero à direita e à esquerda de $RG$, então dizemos que $u$ é **divisor de zero** de $RG$ [1].

Seja $u$ um divisor de zero do anel de grupo $RG$ e, seja $W$ um submódulo de $RG$, com base $S \subseteq G$. O submódulo $Wu$ é chamado de código à esquerda do divisor de zero $u$. No caso em que $RG$ não é comutativo, podemos também definir no anel de grupo o código à direita $uW$. O elemento $u$ é chamado de gerador do código $Wu$ e este submódulo tem base $Su$. Os elementos de $Wu$ são chamados de palavras do código.

Dado $u = \sum_{g \in G} \alpha_g g \in RG$, definimos a RG-matriz associada u, denotada por $M(RG, u)$, como sendo:

$$u = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \cdots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \cdots & \alpha_{g_1^{-1}g_n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \cdots & \alpha_{g_n^{-1}g_n} \end{pmatrix}$$

A matriz $M(RG, u)$ está em $M_{n \times n}(R)$. Note que se $\beta = \sum_{h \in G} \beta_h h \in RG$, o coeficiente de $gh$ do produto $\alpha\beta$ é $(\beta_{h_1}, \beta_{h_2}, \ldots, \beta_{h_n})$ vezes a i-ésima coluna de $M(RG, u)$.

**Teorema:** Dada uma lista dos elementos de um grupo $G$ de ordem $n$, existe um isomorfismo de anéis entre o anel de grupo $RG$ e as $G$-matrizes de tamanho $n \times n$ sobre $R$. Este isomorfismo é dado por $\sigma(w) = M(RG, w)$ [2].

**Exemplo**: O elemento $(1 + R^2) \in \mathbb{Z}_2 D_3$ é um divisor de zero, pois $(1 + R^2)^2 = 0$ e, a matriz associada a ele é dada por:

[1]joao.camargo@ufu.br
[2]alonso.castellanos@ufu.br

$$(1+R^2) = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Pelo teorema acima há um isomorfismo entre os anéis de grupo e o grupo das matrizes $n \times n$. Podemos então, construir a matriz geradora de um código através das matrizes [2].

Seja o $i$-ésimo elemento da lista de elementos do grupo $G$ a identidade do grupo. Então a $i$-ésima linha da matriz do grupo é exatamente a lista de seus elementos, embora, esteja na forma de linha da matriz. Assim, a $i$-ésima linha de cada uma das matrizes dos elementos do anel de grupo, é um vetor que contém todos os outros elementos do anel de grupo, na ordem da listagem tomada.

Agora considere o elemento $g_j u$, onde $g_j$ é o $j$-ésimo elemento da lista do grupo. A matriz do anel de grupo de $g_j u$, é igual ao produto da matriz do anel de grupo $G_j$ de $g_j$ com a matriz do anel de grupo $U$ de $u$. Considere a $i$-ésima linha da matriz $G_j U$. Suas entradas são o produto da linha $i$ de $G_j$ com as colunas de $U$ em ordem. A primeira linha de $G_j$ contém 1 na posição j e, todas as outras entradas serão 0. Assim, a $j$-ésima linha de $U$ deve consistir nos coeficientes de $g_j u$ de acordo com a listagem do grupo.

Com isso, construímos os vetores do código [3].

**Exemplo:** Utilizando a matriz do elemento $(1 + R^2) \in \mathbb{Z}_2 D_3$, tomamos as linhas linearmente independentes obtendo a matriz geradora de um código auto-dual.

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

# Referências

[1] A. S. Castellanos. *Estruturas Algébricas e Aplicações*. Universidade Federal de Uberlândia, Uberlândia, 2017.

[2] T. Hurley. *Group rings and rings of matrices*. Department of Mathematics National University of Ireland, volume 31, 2006.

[3] I. McLoughlin. *Dihedral codes*. National University of Ireland, Galway, 2009.