Homomorfismo de Grupos Cíclicos

Daniela de Oliveira Albanez

Orientador: Prof. Dr. Igor dos Santos Lima

II Workshop de Álgebra da UFG-CAC

e-mail: doalbanez@hotmail.com

Introdução

Inicialmente, relembraremos conceitos básicos da Teoria de Grupos. Posteriormente, tratamos sucintamente sobre homomorfismo de grupos cíclicos, aplicações, teorema do isomorfismo, etc. Nosso objetivo principal é falar sobre homomorfismos de grupos cíclicos, descrevendo $Hom(\mathbb{Z}_n, \mathbb{Z}_m)$ e classificando $Aut(\mathbb{Z}_n)$, a menos de isomorfismos.

Preliminares

Definição. Seja $G \neq \emptyset$: Defina $* : G * G \to G$ por $(a, b) \mapsto a * b$. Dizemos que $(G, *)$ é um grupo se satisfaz:

(i) Associatividade: $(a * b) * c = a * (b * c)$, para quaisquer $a, b, c \in G$;

(ii) Elemento Neutro : $\exists\ e_G \in G : \forall a \in G, e_G * a = a = a * e_G$, para qualquer $a \in G$;

(iii) Elemento Inverso: $\forall a \in G, \exists\ a^{-1} \in G : a * a^{-1} = e_G = a^{-1} * a$.

Observação: G é dito abeliano quando: $a * b = b * a, \forall a, b \in G$.

Exemplo. $G = (\mathbb{z}, +), G = (\mathbb{Q}, +)$.

Definição. Seja $\emptyset \neq H \subseteq G$. Dizemos que H é um subgrupo de G (denotado por $H \subseteq G$) quando H for um grupo com a operação de G restrita para elementos de H. Os grupos G e $\{e_G\}$ são subgrupos do grupo G, são os subgrupos triviais de$G$.

Exemplo. São subgrupos de $\mathbb{z}$ todos os subconjuntos $n\mathbb{z} = \{nx |\ x \in \mathbb{z}\}$, com n inteiro não negativo.

Definição. Se a é elemento de um grupo G, então $< a >= \{a^m \mid m \in \mathbb{z}\}$ é subgrupo de G. Ele é o subgrupo gerado por a. Se $G =< a >$, para algum dos seus elementos, diz-se que G é grupo cíclico.

Exemplo. $\mathbb{z} =< 1 >=< -1 >$,

Definição. Seja $H \leq G$ e $g \in G$. Os subconjuntos de G, $gH = \{gh |\ h \in H\}$ e $Hg = \{hg |\ h \in H\}$ são chamados classe laterais à esquerda e classes laterias à direita de H, respectivamente.

Definição. Dizemos que H é um subgrupo normal de G $(H \triangleleft G)$ quando, $gH = Hg$, $\forall g \in G$.

Definição. Índice de H em G é o número de classes laterias denotado por $[G : H]$.

Teorema (Lagrange).

$$|G| = |H|[G : H].$$

Definição. Sejam $(G_1, *)$ e (G_2, Δ) grupos. Uma função $\varphi : G_1 \to G_2$ é dita um homomorfismo de grupos se tal função preserva a operação dos grupos, isto é, para quaisquer $a, b \in G$ tem-se:
$\varphi(a * b) = \varphi(a)\Delta\varphi(b)$.

Proposição. Seja $\varphi : G_1 \to G_2$ um homomorfismo de grupos. Então:

(i) $)\varphi(e_{G_1}) = e_{G_2}$;

(ii) $\varphi(a^{-1}) = (\varphi(a))^{-1}$;

(iii) se $a \in G_1$ tem ordem m, então a ordem de $\varphi(a)$ divide m.

Definição. Seja $f : G_1 \to G_2$ homomorfismo. $Ker(f) := \{x \in G_1 \mid f(x) = e_{G_2}\}$ é um subgrupo normal de G_1, chamado núcleo do homomorfismo de f.

Definição. Seja $f : G_1 \to G_2$ homomorfismo.

$Im(f) := \{y \in G_2 \mid y = f(g), \text{ algum } g \in G_1\}$

é um subgrupo de G_2, chamado imagem de f.

Teorema (Isomorfismo). Seja $f : (G_1, *) \to (G_2, \Delta)$ um homomorfismo de grupos. Então, $\frac{G_1}{Ker(f)} \cong Im(f)$.

Definição. Dizemos que $f : G_1 \to G_2$ é um automorfismo quando f é um homomorfismo, f é bijetivo e $G_1 = G_2$.

Resultados

Lemma. Se G é um grupo cíclico então $Aut(G)$ é um grupo abeliano.

Demonstração. Seja G um grupo cíclico e seja g um gerador de G. Considerando $f_1, f_2 \in Aut(G)$, queremos mostrar que $f_1 f_2 = f_2 f_1$. Para isto é suficiente mostrarmos que $(f_1 f_2)(g) = (f_2 f_1)(g)$. Suponha que $f_1(g) = g^r$ e $f_2(g) = g^s$. Assim $(f_1 f_2)(g) = f_1(f_2(g)) = f_1(g^s) = f_1(g)^s = g^{rs}$ e $(f_2 f_1)(g) = f_2(f_1(g)) = f_2(g^r) = f_2(g)^r = g^{rs}$. como queríamos demonstrar. □

Vamos resolver $Hom(\mathbb{Z}_n, \mathbb{Z}_m)$. Um homomorfismo $f \in Hom(\mathbb{Z}_n, \mathbb{Z}_m)$ é tal que se $g \in \mathbb{Z}_n$ e a ordem de g é finita, então $|f(g)| \mid |g|$. No caso de f ser um isomorfismo, temos que $|g| = |f(g)|$. Portanto, no cálculo do $Hom(\mathbb{Z}_n, \mathbb{Z}_m)$ é necessário você saber os geradores de $\mathbb{Z}_n$ e as ordens dos elementos de $\mathbb{Z}_m$. Nem todo elemento de $\mathbb{Z}_m$ precisa ser atingido, pois nem todo homomorfismo de $Hom(\mathbb{Z}_n, \mathbb{Z}_m)$ é sobrejetivo.

Exemplo.

(1) O homomorfismo trivial, que leva todo elemento de $\mathbb{Z}_n$ na identidade de $\mathbb{Z}_m$, não é um homomorfismo sobrejetivo se $|G| > 1$.

(2) $Hom(\mathbb{Z}_3, \mathbb{Z}_2)$. Como 1 gera $\mathbb{Z}_3$ (logo tem ordem 3), precisamos agora saber as ordens dos elementos de $\mathbb{Z}_3$ e as ordens dos elementos de $\mathbb{Z}_2$. Qualquer homomorfismo $f \in Hom(\mathbb{Z}_3, \mathbb{Z}_2)$ levará $1 \in \mathbb{Z}_3$ em algum elemento de $\mathbb{Z}_2$ que tenha ordem 1 ou 3. Ou seja, as únicas ordens do contradomínio que nos interessam são essas possíveis. Mas em $\mathbb{Z}_2$ só temos elementos de ordem 1 (só o 0) ou 2 (só o 1). Logo os elementos de $Hom(\mathbb{Z}_3, \mathbb{Z}_2)$ é o seguinte homomorfismo: $f_1 =$ homomorfismo trivial, isto é leva $1 \in \mathbb{Z}_3$ em $0 \in \mathbb{Z}_2$ que é o elemento identidade de $\mathbb{Z}_2$.

Para conhecermos os grupos de automorfismos de grupos cíclicos, devemos estudar $Aut(\mathbb{Z}_n)$. Para determinar o $Aut(\mathbb{Z}_n)$, basta ter em mente que isomorfismo leva gerador em gerador e portanto elementos de mesma ordem vão em elementos de mesma ordem. Em $Aut(\mathbb{Z}_n)$ todo homomorfismo f leva 1 em algum outro possível gerador, isto é, em algum número entre 1 e $n-1$ que seja coprimo com n. Logo, temos que $|Aut(\mathbb{Z}_n)|$ corresponde a quantidade de números coprimos com n entre 1 e n. Em particular, se $n = p$ com p primo, então todo número entre 1 e $p-1$ é coprimo com p. Logo $|Aut(\mathbb{Z}_p)| = p-1$.

Referências

[1] GARCIA, Arnaldo e LEQUAIN, Yves, *Elementos de Álgebra. IMPA*, 6º ed. Rio de Janeiro. 2012

[2] LIMA, Igor, *Dicas para a 6ª Lista de Álgebra 1 (Conteúdo: Homomorfismo de Grupos e Teorema do Isomorfismo para grupos).*

Este projeto foi financiado pela FAPEG através do edital 05/2013 para realização de eventos.