[Grupo]

0.1 Definições e Propriedades

Daremos uma definição inicial em termos de objetos já trabalhados:

Def. 0.1. Um grupo é um grupóide com um único objeto.

Isto é, um grupóide com um único objeto é uma categoria na qual, denominando por φ esse único objeto, então $\mathrm{Aut}_(\varphi)$ carrega toda informação sobre ela. Denominamos assim um grupo $G = Aut_(\varphi)$. Assim, diretamente, vemos que pela definição de categoria temos a existência de uma identidade, sobre uma operação associativa (i.e morfismos), além disso como todo morfismo é iso, temos também a existência da inversa.

Dada essa prévia discussão, em termos usuais, podemos pensar em um grupo como um conjunto munido de uma operação obedecendo certos axiomas, isto é:

Def. 0.2 (Grupo)**.** Seja G um conjunto não vazio, munido de uma operação binária $\cdot : G \times G \to G$ denotado pela tupla $(G, \cdot)$, então G é um grupo caso:

- A operação $\cdot$ é associativa, ou seja:

$$\forall g, h, k \in G, (g \cdot h) \cdot k = g \cdot (h \cdot k)$$

- Existência da identidade e_G para a operação:

$$\exists e_G \in G \forall g \in G, g \cdot e_g = e_g \cdot g = g$$

- Existência da identidade:

$$\forall g \in G, \exists h \in G, hg = gh = e_G$$

Exercício 0.1. Mostre que as duas definições são de fato equivalentes, isto é mostre que todo grupo pode ser escrito como o grupo de automorfismos de algum objeto em uma categoria.

Resp. 0.1. Seja G um grupo. Construímos a categoria da seguinte forma: Tome $() = e_G$. e considere

Com essas diferentes visões sobre um grupo dadas, podemos começar a tentar obter propriedades interessantes sobre essas estruturas, assim:

Prop. 0.1. A identidade é única. Isto é, se $h \in G$ é uma identidade, então $h = e_G$ assim concluímos que todo grupo possuí ao menos um elemento especial bem definido.

Prop. 0.2. Por inspeção:

$$h = e_G h = e_g$$

Prop. 0.3. Elementos inversos também são únicos.

Demonstração. Tome $g \in G$ e $h_1, h_2 \in G$ inversos de g, novamente, por inspeção:

$$h_1 = e_G h_1 = h_2(h_1 g) = h_2$$

□

Prop. 0.4. Seja $(G, \cdot)$ um grupo. Então $\forall a, g, h \in G\ ga = ha \implies g = h, ag = ah \implies g = h$.

Demonstração. Novamente, por inspeção:

$$ga = ha \implies (ga)a^{-1} = (ha)a^{-1} \implies g = h$$

. Da mesma forma, concluímos o mesmo para o outro fato. □

Grupos comutativos

Até agora em nenhum momento exigimos que elementos de um grupo comutem sobre a operação, nem sequer definimos o significado de "comutar", entretanto grupos comutativos são de extrema importância matemática. Assim:

Def. 0.3. Dizemos que um grupo é comutativo (ou abeliano) se:

$$\forall g, h \in G, gh = hg$$

Quando um grupo é abeliano, mudamos nossa terminologia. Usualmente se trata a operação conforme uma adição, denotando a identidade como 0_G, $\cdot$ como $+$ e a inversa de a por $-a$.

Ordem

Def. 0.4. Um elemento $g \in G$ possuí ordem finita se $g^n = e$ para algum n inteiro positivo. Nesse caso, a ordem $|g|$ é o menor inteiro n tal qual isso é observado.

Dessa definição abstraímos diretamente:

Lemma 0.1. *Se $g^n = e$ para algum n inteiro, então $|g|$ divide n.*

Lemma 0.2. *Temos que $g^n = e$, para $m = |g|$, $g^m = e$ tal qual $(g^m)^p = e, \forall p \in \mathbb{Z}^+$ com necessariamente $(g^m)^q = (g^n)$ para algum q, já que caso contrário, podemos verificar m não seria o menor inteiro assim diretamente $n = m * q$, portanto $m$divide $n \iff |g|$divide n.*

Def. 0.5. Se G enquanto conjunto é finito, então a ordem $|G|$ de G é sua cardinalidade, caso G é infinito, então $|G| = \infty$

Dessa definição podemos concluir que $|g| \leq |G|, \forall g \in G$, já que no caso finito (infinito é vacuosamente verdadeiro) para todo $g \in G$, se $n = |G|$ então

$(g^0, ..., g^n)$ não podem ser todos distintos como consequência direta dessa finitude, então, $\exists i, j : 0 \leq i < j \leq |G|$, assim $g^i = g^j \implies g^{j-i} = e$. Dessa forma $|g| \leq (j - i) \leq |G|$.

Desse fato, concluímos também que se g possuí ordem finita, então $g^m, \forall m \geq 0$ também e:

$$|g^m| = \frac{\text{lcm}(m, |g|)}{m} = \frac{|g|}{\text{gcd}(m, |g|)}$$

Tal conclusão segue do fato que inicalmente $\text{lcm}(a, b) = ab/\text{gcd}(a, b), \forall a, b$. Assim é necessário mostrar que $|g^m| = \frac{\text{m, —g—}}{m}$. Assim, tome d tal qual $g^{md} = e$, ou seja d tal qual $md = \alpha|g|$, dessa forma por essa definição $m|g^m|$ é o menor multiplo de m e de $|g|$ assim, $m|g^m| = \text{lcm}(m, |g|)$, concluindo o nosso objetivo.

Em geral, para elementos comutativos, $gh = hg \implies |gh|$ divide $\text{lcm}(|g|, |h|)$. O que pode ser demonstrado tomando $|g| = m, |h| = n$ tal qual se N é múltiplo comum de m, n então $g^N = h^N = e$

0.2 Exemplos de Grupos

Def. 0.6 (Grupos Simétricos)**.** Seja A um conjunto. O grupo simétrico, ou grupo de permutações de A é o grupo $\text{Aut}_{\mathfrak{Set}}(A)$. O grupo de permutações do conjunto $\{1, ..., n\}$ é denotado por S_n

Essa ideia de permutação pode ser observada mais claramente, ao observar o comportamento desse conjunto de automorfismos. Inicialmente fixamos um conjunto A, temos então que como $= \mathfrak{Set}$, $\text{Aut}(A)$ são simplesmente as bijeções de A para A, ou seja, suas permutações, cuja simetria está ligado a uma apenas "reordenação"do conjunto preservando sua propriedades.

Nessa definição, algo que deixou-se de lado a forma em que pensamos no produto $\cdot$. Na visão categorial, a definição direta advém da composição de morfismos, isto é defimos:

$$f \cdot g := \forall p \in A, g \circ f(p) = g(f(p)).$$

Um jeito de pensar nos elementos dos grupos S_n, é utilizando a notação por matrizes $2 \times n$ com $f \in Aut_{\mathfrak{Set}}(A)$:

$$a_{ij} = \Big\{ i = 1, a_{ij} = ji = 2, a_{ij} = f(j)$$

De forma auxiliar a visualização. Podemos pensar também no produto como $\forall p \in A, fp = (p)fp$, nessa notação também sendo facilitado.

Dando atenção em específico a S_3 vemos que enquanto conjunto ele é dado por:

$$\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}$$

Exercício 0.2. Mostre que para $n \geq 3, S_n$ não é comutativo.

Def. 0.7 (Grupos diedrais)**.** Grupos surgem naturalmente no contexto de simetrias, imediatamente a partir da definição. Isto é, formalmente, pensamos em simetrias como transformações que preservam certas propriedades de um objeto matemático, isto é, automorfismos de dado objeto de uma categoria.

Assim, no contexto de figuras geométricas (planas) surge o conceito de grupos diedrais, tal qual definimos grupos diedrais como o conjunto de todas transformações espaciais que ocasionam em simetriais (movimentos rigidos).

Assim, para um polígono regular de n lados centrado na origem, seu grupo simétrico é composto por n rotações de $\frac{2\pi}{n}$ ao longo da origem e n reflexões dadas por seus eixos de simetria. Dessa forma denominamos o grupo de simetrias associadas a um polígono regular de n lados como D_{2n}.

É interessante ver que, dessa definição, concluímos diretamente que há uma relação entre grupos diedrais e simétricos, isto é, mais especificamente, existe uma função $f : D_{2n} \to S_n$, injetiva (confira!), basta ver que D_{2n} pode ser caracterizado enumerando cada vertice e suas transformações simétricas, que devem ser um subconjunto das permutações possíveis. Mais adiante trataremos tais casos com mais rigor e generalizações.

Def. 0.8 (Grupos Cíclicos)**.** Iniciamos esse caso, tomando a seguinte relação de equivalência:

$$(\forall a, b \in \mathbb{Z}) : a \equiv b \mod n \iff n|(b-a)$$

Denominada congruência módulo n, denotada por n É evidente que n possuí n elementos (restos possíveis para essa divisão):

$$[0]_n, [1]_n, ..., [n-1]_n$$

Definimos assim, a relação binária nesse conjunto $+ : n \times n \to n, \forall a, b \in \mathbb{Z}, [a] + [b] := [a + b]$, de modo a obter um grupo a partir dessa estruturas (verifique!).

É evidente ainda, como essa operação herda propriedades de $\mathbb{Z}$, esse grupo é abeliano