Algebra, Chapter 0: Anotações

Pedro Saccomani

Dezembro de 2022

1 Preliminares

1.1 Princípios de Teoria de Conjuntos

Antes de iniciar a discussão, é interessante tratar algumas definições básicas e iniciais, assim temos:

Definição 1.1 (Relação de Equivalência)**.** Uma relação de equivalência sobre um conjunto S é uma relação que obedece as seguintes propriedades:

- Reflexividade: $(\forall a \in S) a \sim a$.
- Simetria: $(\forall a \in S)(\forall b \in S) a \sim b \implies b \sim a$
- Transitividade: $(\forall a, b, c \in S)(a \sim b \text{ and } b \sim c) \implies a \sim c$

Dessa definição surge a possibilidade de se obter uma partição de S. Assim, se $\forall a \in S$ a classe de equivalência de a é definida como:

$$[a]_\sim := \{b \in S | b \sim a\}$$

Exercício 1.1. Mostre que as classes de equivalência formam uma partição $\mathcal{P}_\sim$ de S

Resposta 1.1. Para demonstrar esse item queremos mostrar que cada conjunto da classe $\mathcal{P}_\sim$ são disjuntos dois a dois, e $\bigcup \mathcal{P} = S$.

Dessa forma, tomando $A, B \in \mathcal{P}_\sim$, tal qual $A \cap B \neq \emptyset$, temos $\exists x \in A \cap B$ tal qual, $\forall y \in A, x\ y \implies y \in B \implies A \subset B$ e $\forall \overline{y} \in B, x\ \overline{y} \implies \overline{y} \in A \implies B \subset A \therefore A = B$. Assim, de fato, todo conjunto nessa classe deve ser disjunto entre sí.

É evidente que $\bigcup \mathcal{P} = S$, diretamente da definição de classes de equivalência.

Exercício 1.2. Mostre que cada partição $\mathcal{P}$ possuí uma relação de equivalência correspondente, concluindo assim, que as noções de partição e relação de equivalência são as mesmas.

A partir dessa ideia de que a classe de conjuntos formada pelas classes de equivalência de S formam uma partição, podemos partir para a ideia de operação de quociente em um conjunto:

Definição 1.2 (Quociente)**.** Seja S um conjunto, então seu quociente em respeito a relação de equivalência $\sim$ é o conjunto:

$$S/\sim := \mathcal{P}_\sim$$

Exemplo 1.1. Seja $S = \mathbb{Z}$ e $\sim$ definida por:

$$a \sim b \iff a - b \text{ é par.}$$

Então $\mathbb{Z}/\sim$ consiste das duas classes de equivalência, nominalmente:

$$\mathbb{Z}/\sim = \{[0]_\sim, [1]_\sim\}.$$

Que em linhas gerais, "separa"os inteiros em pares e ímpares (motivação para aritmética modular).

Uma forma de se pensar sobre a operação de quociente, é que neste novo conjunto, a relação de equivalência se torna uma igualdade nesse conjunto.

1.2 Funções entre conjuntos

Além dos exemplos já conhecidos e tratados, temos também algumas "novas"noções, tais quais:

Definição 1.3 (Monomorfismo)**.** Uma função $f : A \to B$ é um monomorfismo (ou *monic*) se para todos conjuntos Z e todas funções $\alpha', \alpha'' : Z \to A$, $f \circ \alpha' = f \circ \alpha'' \implies \alpha = \alpha''$

Proposição 1.1. Uma função é injetiva se só se é um monomorfismo.

Demonstração. ($\implies$) Sabemos que uma função $f : A \to B$, é injetiva então possuí inversa à esquerda, i.e $\exists g, g \circ f = id_A$. Assim, seja $\alpha'', \alpha'', Z \to A, f \circ \alpha' = f \circ \alpha''$. Da hipótese e do resultado enunciado, tomando a composição dessa construção por g, e a associatividade:

$$(g \circ f) \circ \alpha' = (g \circ f) \circ \alpha''$$

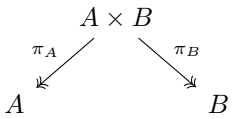
Assim, $id_A \circ \alpha' = id_A \circ \alpha'' \implies \alpha' = \alpha''$. Assim, concluímos f é um monomorfismo.

Para a ($\impliedby$) partimos de uma f monomorfismo. Pela definição podemos tomar $Z = \{p\}$ para um dado p, e $\alpha', \alpha'' Z \to A$.

Para toda temos que se $\alpha'' = \alpha''$ então para qualquer escolha de $\alpha'(p), \alpha''(p)$, vale que $f(\alpha') = f(\alpha'') \implies \alpha' = \alpha''$. Pela contrapositiva, i.e $\alpha' \neq \alpha'' \implies f(\alpha') \neq f(\alpha'')$. Assim, f deve ser injetiva. □

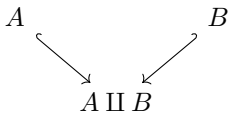
Exercício 1.3. Formule a noção de epimorfismo de maneira análoga a de monomorfismo e formule e demonstre um resultado análogo ao anterior.

Exemplo 1.2. Sejam A e B dois conjuntos. Então temos as projeções naturais, π_A, π_B:



Definidas por $\pi_A = ((a,b)) := a, \pi_B((a,b)) := b, \forall (a,b) \in A \times B$. Tais quais por definição são sobrejetores.

Exemplo 1.3. Similarmente, existem funções injetoras naturais de A para B para a união disjunta (denotada aqui por $\amalg$):



Obtida ao associar cada elemento de $a, b \in A, B$ a seus respectivos elementos de $A + B$.

Exemplo 1.4. Seja $\sim$ uma relação de equivalência sobre um conjunto A, então existe uma projeção canônica, sobrejetora:

$$A \longrightarrow\!\!\!\!\!\rightarrow A/\sim$$

Obtido ao associar todo $a \in A$ a sua classe de equivalência $[a]_\sim$.

Até agora foi dada uma clara enfâse aos mapas injetores e sobrejetores, isso ocorre pois elas conferem os "blocos"construtores necessários para qualquer função. Para observar este fato, basta observar que cada função $f : A \to B$ determina uma relação de equivalência em A tal qual $\forall \alpha', \alpha'' \in A$,'

$$\alpha' \sim \alpha'' \iff f(\alpha') = f(\alpha'').$$

Proposição 1.2. Seja $f : A \to B$ uma função, e $\sim$ uma relação de equivalência.

Então f pode ser decomposta como: $A \longrightarrow\!\!\!\!\!\rightarrow (A/\sim) \xrightarrow[\tilde{f}]{\sim} \mathrm{Im}f \hookrightarrow B$, com $A \to B$ dado por f.

Onde a primeira função é a projeção canônica e a terceira a operação de inclusão e $\tilde{f}$, bijeção é definida como $\tilde{f}([a]_\sim) := f|(a)$

1.3 Categorias

No contexto atual, vemos a necessidade de dar importância a como dois diferentes objetos podem se relacionar, como já dada a motivação por conjuntos. Assim, urge a ideia de pensar em categorias.

Definição 1.4 (Categorias)**.** De forma direta, uma categoria $\mathfrak{C}$ consiste em uma coleção (classe) de objetos $\mathrm{Obj}\mathfrak{C}$ e morfismos entre eles, isto é para todo A, B de $\mathfrak{C}$, temos um conjunto $\mathrm{Hom}_\mathfrak{C}(A, B)$ de morfismos com as seguintes propriedades:

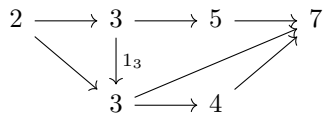
- Existência da identidade: Para todo objeto A de $\mathfrak{C}$ existe ao menos um morfismo $1_A \in \mathrm{Hom}_{\mathfrak{C}}(A, A)$.
- Composição de morfismos: Sejam $f \in \mathrm{Hom}_{\mathfrak{C}}(A, B), g \in \mathrm{Hom}_{\mathfrak{C}}(B, C)$ então $gf \in \mathrm{Hom}_{\mathfrak{C}}(A, C)$. Ou seja para toda tripla de objetos $A, B, C, \exists$ h tal qual:
$$h : \mathrm{Hom}_{\mathfrak{C}}(A, B) \times \mathrm{Hom}_{\mathfrak{C}}(B, C) \to \mathrm{Hom}_{\mathfrak{C}}(A, C)$$
- Composição é associativa, isto é, se $f \in \mathrm{Hom}_{\mathfrak{C}}(A, B), g \in \mathrm{Hom}_{\mathfrak{C}}(B, C), h \in Hom_{\mathfrak{C}}(C, D)$, então:
$$(hg)f = h(gf).$$
- As identidade são identidades em relação a composição, isto é para todo $f \in \mathrm{Hom}_{\mathfrak{C}}(A, B)$
$$f1_A = f = 1_B f$$
- Se $A \neq B, B \neq D$ então $\mathrm{Hom}_{\mathfrak{C}}(A, B), \mathrm{Hom}_{\mathfrak{C}}(C, D)$ são disjuntos;

Denominamos como *endomorfismo* um morfismo de uma objeto A da categoria para sí mesmo, assim $\mathrm{Hom}_{\mathfrak{C}}(A, A)$ é denotado por $\mathrm{End}_{\mathfrak{C}}(A)$.

Exemplo 1.5. Denotaremos, aqui como $\mathfrak{Set}$ a categoria de todos conjuntos, assim:

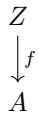
- Obj($\mathfrak{Set} =$) classe de todos conjuntos.
- Para $A, B \in \mathrm{Obj}(\mathfrak{Set})$, então $\mathrm{Hom}_{\mathfrak{Set}(A,B)} = B^A$

Exemplo 1.6. Considere a categoria $\mathfrak{C}$ que abriga gerada a partir de $\mathbb{Z}$ munida da relação de equivalência $\leq$, como o dado seguinte diagrama *comutativo*:

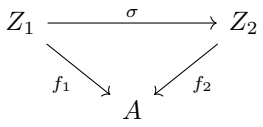


Exemplo 1.7 (Slice Category). Seja $\mathfrak{C}$ uma categoria, e A um objeto de C. Definimos a categoria $\mathfrak{C}_A$ com seus objetos sendo certos morfismos de $\mathfrak{C}$ e seus morfismos correspondentes, diagramas de $\mathfrak{C}$, isto é:

- Obj($\mathfrak{C}_A$) = todos morfismos de qualquer outro objeto de $\mathfrak{C}$ para A, i.e, qualquer objeto de $\mathfrak{C}_A$ é um morfismo $f \in \mathrm{Hom}_{\mathfrak{C}}(Z, A)$ para algum Z de $\mathfrak{C}$, em um diagrama:



- Os morfismos dessa categoria podem ser representador pelo seguinte diagrama, onde f_1, f_2 são objetos dela:

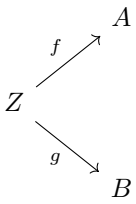


Tal qual σ representa o morfismo $f_1 \to f_2$, com $\mathfrak{C}_A$ denominada a categoria ambiente de $\mathfrak{C}$.

Exercício 1.4. Verifique que a categoria descrita anteriormente obedece os respectivos axiomas.

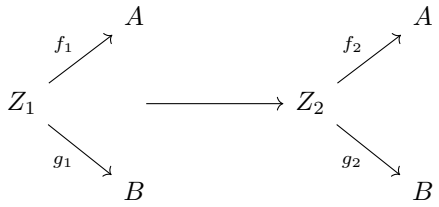
Exemplo 1.8. Seja $\mathfrak{C}$ uma dada categoria, e A, B dois objetos da mesma. Podemos definir uma categoria $C_{A,B}$ da mesma maneira que definimos no último exemplo, isto é:

- Obj($\mathfrak{C}_{A,B}$) são os diagramas:

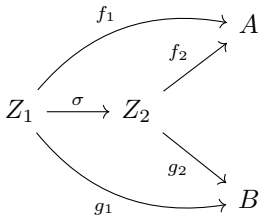


Isto é, Obj$\mathfrak{C}_{A,B}$ são simplesmente as tuplas formadas tomando para todo objeto Z de $\mathfrak{C}$, $f \in \mathrm{Hom}(Z, A), g \in \mathrm{Hom}(Z, B), (f, g)$.

- Seus morfismos podem ser representados pelos diagramas:



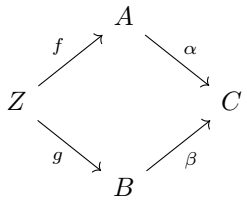
Que equivalem ao seguinte diagrama comutativo:



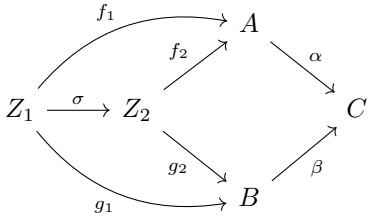
Formalmente podemos pensar nesses diagramas como a definição, tomando dois objetos C, Dde $\mathfrak{C}_{A,B}$, com C, D sendo morfismos de dado Z_1, Z_2 para A, B de $\mathfrak{C}$, com $C = (f_1, g_1), D = (f_2, g_2)$ tal qual $Hom(C, D) = \sigma : Z_1 \to Z_2$ tal qual $f_1 = f_2\sigma$ e $g_1 = g_2\sigma$

Exemplo 1.9. Trataremos aqui de $\mathfrak{C}^{A,B}$. Seja $\mathfrak{C}$ e fixe dois morfismos $\alpha : A \to C, \beta : B \to C$ em $\mathfrak{C}$. Então considere a categoria determinada por:

- $\mathrm{Obj}(\mathfrak{C}_{\alpha,\beta})$ os diagramas comutativos:



- Os morfismos determinados pelo seguinte diagrama:



Exercício 1.5. Seja $\mathfrak{C}$ uma categoria. Considere a estrutura $\mathfrak{C}^{op}(A, B)$ com:

- $\mathrm{Obj}(\mathfrak{C}^{op}) := \mathrm{Obj}(\mathfrak{C})$;
- Para A, B objetos de $\mathfrak{C}^{op}$, $\mathrm{Hom}_{\mathfrak{C}^{op}}(A, B) := \mathrm{Hom}_{\mathfrak{C}}(B, A)$.

Mostre como formalizar essa estrutura em uma categoria, isto é defina a composição de morfismos e verifique os axiomas necessários.

Exercício 1.6. Seja A um conjunto finito, então quão grande é $End_{\mathfrak{Set}}(A)$?

Resposta 1.2. O conjunto de morfismos na categoria $\mathfrak{Set}$ consiste em todas funções $f : S \to \tilde{S}$ com $S, \tilde{S}$. Assim, podemos pensar em no conjunto de endomorfismos de um dado A de cardinalidade finita, como permutações para todos subconjuntos deles. Isto é, denotando M como esse valor:

$$M = (|A|)^{|A|}$$

Tratando esse problema com um de contagem, onde basicamente cada elemento do conjunto pode ser e para qualquer outro.

Exercício 1.7. Seja V uma categoria com $\mathrm{Obj}(V) = \mathbb{N}$, com $\mathrm{Hom}(n, m)$ o conjunto das matrizes $m \times n$ com valores reais.

1.4 Morfismos

Definição 1.5 (Isomorfismo)**.** Um morfismo $f \in \mathrm{Hom}_{\mathfrak{C}}(A, B)$ é denominado isomorfismo se possuí uma inversa por ambos lados, isto é $\exists g \in \mathrm{Hom}_c(B, A)$ tal qual:

$$gf = 1_A, fg = 1_B$$

Proposição 1.3. A inversa de um isomorfismo é única.

Demonstração. Queremos mostrar que se $g_1, g_2 : B \to A$ atuam como inversas de um isomorfismo $f : A \to B$ então $g_1 = g_2$. Assim:

$$g_1 = g_1 1_B = g_1(fg_2) = (g_1 f)g_2 = g_2$$

□

Proposição 1.4. As seguintes afirmações são verdadeiras:

- Toda identidade 1_A é um isomorfismo e sua própria inversa.
- Se f é um isomorfismo, então f^{-1} também é, tal qual $(f^{-1})^{-1} = f$.
- Se $f \in \mathrm{Hom}_{\mathfrak{C}}(A, B), g \in \mathrm{Hom}_{\mathfrak{C}}(B, C)$ são isomorfismos, então sua composta gf também é, de inversa $f^{-1}g^{-1}$.

Demonstração. Basta inspecionar as afirmações. □

Exemplo 1.10 (Grupóide). De maneira lúdica, podemos pensar em um grupóide como uma categoria, tal qual todos seus morfismos são iso.

Um automorfismo de um objeto A de uma categoria $\mathfrak{C}$ é um iso de $A \to A$, tal qual diretamente $\mathrm{Aut}_{\mathfrak{C}}(A) \subset \mathrm{End}_{\mathfrak{C}}(A)$. É possível verificar de forma direta, que $\mathrm{Aut}_{\mathfrak{C}}(A)$ é fechado para composição, que por sua vez é associativa, além disso contém a identidade, e toda inversa.

Assim, para toda categoria e seus objetos, esse conjunto é grupo.

Acima, tratamos da importante noção de isomorfismos, conforme já realizado anteriormente.

Partimos, agora, para a definição em termos categóricos de estruturas já trabalhadas anteriormente.

Definição 1.6 (Monomorfismo)**.** Seja $\mathfrak{C}$ uma categoria. Um morfismo entre objetos A, B é um monomorfismo se para todo objeto Z de $\mathfrak{C}$ e todos morfismos α', α'' entre Z, A:

$$f \circ \alpha' = f \circ \alpha'' \implies \alpha' = \alpha''$$

Definição 1.7 (Epimorfismo)**.** Seja $\mathfrak{C}$ uma categoria. Um morfismo entre objetos A, B é dito epimorfismo se para todo objeto Z e todos morfismos β', β'' entre B, Z:

$$\beta' \circ f = \beta'' \circ f \implies \beta' = \beta''$$

1.5 Propriedades Universais

Até agora, o nosso estudo em categorias tratou de diversos casos específicos, entretanto, como categorias são objetos matemáticos extremamente gerais, naturalmente a idea de um tratamento mais universal se torna presente. Assim, iniciando com definições amplas:

Definição 1.8 (Objeto Inicial)**.** Seja $\mathfrak{C}$ uma categoria. Dizemos que um objeto I de $\mathfrak{C}$ é inicial em $\mathfrak{C}$ se para todo objeto A de C existe um único morfismo $I \to A$. i.e:

$$\forall A \in \mathrm{Obj}(\mathfrak{C}) : |\mathrm{Hom}_{\mathfrak{C}}(I, A)| = 1$$

Definição 1.9. Dizemos que um objeto F de $\mathfrak{C}$ é final se:

$$\forall A \in \mathrm{Obj}(\mathfrak{C}) : |\mathrm{Hom}_{\mathfrak{C}}(A, F)| = 1$$

Se um objeto satisfaz qualquer uma dessas duas propriedades, dizemos que ele é um objeto terminal.

Essa definição extremamente simples, nós traz uma propriedade relativamente forte. Em linhas gerais, queremos mostrar que são únicos a menos de isomorfismo único, isto é, formulamos:

Proposição 1.5. Seja $\mathfrak{C}$ uma categoria, então:

- Se I_1, I_2 são objetos iniciais em $\mathfrak{C}$, então $I_1 \backsimeq I_2$.
- Se F_1, F_2 são objetos finais em $\mathfrak{C}$ então $F_1 \backsimeq F_2$

Demonstração. Sejam I_1, I_2 dois objetos iniciais de $\mathfrak{C}$ então, $\exists! f : I_1 \to I_2$, $\exists! g : I_2 \to I_1$, além disso o único endomorfismo de I_1, I_2 é a identidade, por definição. Dessa forma $fg = 1_{I_2}$ e $gf = 1_{I_1}$, assim $f : I_1 \to I_2$ é um isomorfismo.

De mesma maneira, podemos concluir o mesmo fato para objetos finais. □

Objetos terminais desempenham um papel fundamental em certas propriedades universais. Os seguintes tópicos exibirão isso (em geral ligamos propriedades universais com objetos terminais).

Quociente

Seja $\sim$ uma relação de equivalência em um conjunto A. Queremos entender a afirmação "O quociente $A/\sim$ é universal em relação a propriedade de mapear A para um conjunto de forma que elementos equivalente possuem a mesma imagem, isto é:

$$A \xrightarrow{\varphi} Z$$

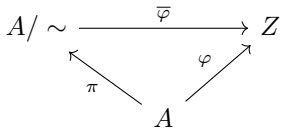
Para qualquer Z no qual:

$$a' \sim a'' \implies \varphi(a') = \varphi(a'')$$

Definimos assim, a categoria $\mathfrak{C}'$ denotada por (φ, Z), queremos saber se essa categoria possuí objetos iniciais.

Proposição 1.6. Seja π a projeção canônica, o par $\pi, A/\sim$ é um objeto inicial dessa categoria.

Demonstração. Considere φ, Z definido acima. Queremos que o diagrama:



Seja único, i.e $\exists!\overline{\varphi}$. Como estamos numa categoria, o diagrama comuta tal qual:

$$\overline{\varphi}([a]_\sim) = \varphi(a)$$

Ou seja, $\overline{\phi}$ é de fato única para todo Z.

Assim, por fim, é preciso que $\overline{\varphi}$ seja bem definida. De fato:

$$[a_1]_\sim = [a_2]_\sim \implies a_1 \sim a_2 \implies \phi(a_1) = \phi(a_2)$$

Logo, como queríamos mostrar, esse objeto é inicial. □

Produto

Partindo da ideia de produto de conjuntos, queremos obter um conceito mais geral que possa ser observado em qualquer categoria. Com isso, temos a seguinte ideia: O produto de dois conjuntos A, B (com suas respectivas projeções naturais) é um objeto final na categoria $\mathfrak{C}_{A,B}$.

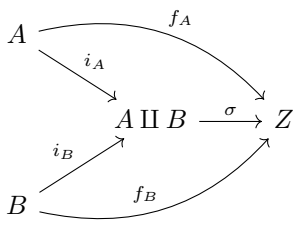
Dizemos ainda que uma categoria $\mathfrak{C}$ possuí produtos finitos se $\forall A, B \in \mathfrak{C}, \mathfrak{C}_{A,B}$ possuí objetos finais tal qual existam dois morfismos $A \times B \to A, A \times B \to B$

Exercício 1.8. Mostre que o produto cartesiano entre conjuntos A, B obedece essa propriedade em $\mathfrak{C} = \mathfrak{Set}$

Coprodutos

Intuitivamente pensamos pelo prefixo *co-* que estes seriam o "inverso"do caso anterior, isto é, mais claramente:

Definição 1.10 (Coproduto)**.** Definimos como coproduto de dois objetos A, B de uma categoria $\mathfrak{C}$, os objetos iniciais da categoria $\mathfrak{C}^{A,B}$, tal qual, no diagrama abaixo, para o coproduto $A \amalg B$ é um objeto de $\mathfrak{C}$ munido de $\exists!\sigma : A \amalg B$



Proposição 1.7. A união disjunta em $\mathfrak{Set}$ é um coproduto.

Demonstração. Definimos a união disjunta de conjuntos A, B como a união de seus pares isomorfos disjuntos, A', B'. Assim, tomando $A' = 0 \times A, B' = 1 \times B$, com $i_A(a) = i(0, a), i_B(b) = (1, b)$. Note que esse é um caso específico, mas não precisamos tratar em geral, já que qualquer outra união disjunta será isomorfa a essa definição.

Assim simplemente da definição,

$$\sigma(c) = \begin{cases} f_A(a), \text{se } c & = (0, a) \in \{0\} \times A \\ f_B(b), textsec & = (1, b) \in \{1\} \times B \end{cases}$$

Tal qual a comutatividade e unicidade são diretas. □

2 Primeiro encontro com Grupos

2.1 Definições e Propriedades

Daremos uma definição inicial em termos de objetos já trabalhados:

Definição 2.1. 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 $\mathrm{Aut}_{\mathfrak{C}}(\varphi)$ carrega toda informação sobre ela. Denominamos assim um grupo $G = Aut_{\mathfrak{C}}(\varphi)$. 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:

Definição 2.2 (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 inversa:

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

Exercício 2.1. 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.

Resposta 2.1. Seja G um grupo. Construímos a categoria $\mathfrak{C}$ da seguinte forma: Tome $\mathrm{Obj}(\mathfrak{C}) = e_G$. e considere

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

Proposição 2.1. 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.

Demonstração. Por inspeção:

$$h = e_G h = e_g$$

□

Proposição 2.2. Elementos inversos também são únicos.

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

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

□

Proposição 2.3. 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:

Definição 2.3. 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

Definição 2.4. 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:

Lema 2.1. *Se $g^n = e$ para algum n inteiro, então $|g|$ divide n.*

Lema 2.2. *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.*

Definição 2.5. 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:

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

Tal conclusão segue do fato que inicalmente $\operatorname{lcm}(a, b) = ab/\gcd(a, b), \forall a, b$. 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, $m|g^m| = \operatorname{lcm}(m, |g|)$, concluindo o nosso objetivo.

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

2.2 Exemplos de Grupos

Definição 2.6 (Grupos Simétricos)**.** Seja A um conjunto. O grupo simétrico, ou grupo de permutações de A é o grupo $\operatorname{Aut}_{\mathfrak{Set}}(A)$. 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 $\mathfrak{C} = \mathfrak{Set}$, $\operatorname{Aut}(A)$ 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 2.2. Mostre que para $n \geq 3, S_n$ não é comutativo.

Definição 2.7 (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.

Definição 2.8 (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 $\mathbb{Z}/n\mathbb{Z}$ É evidente que $\mathbb{Z}/n\mathbb{Z}$ possuí n elementos (restos possíveis para essa divisão):

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

Definimos assim, a relação binária nesse conjunto $+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \forall a, b \in \mathbb{Z}, [a] + [b] := [a + b]$, 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.

Grupos cíclicos terão maior enfase posteriormente, mas sua importância deve ser claramente notada, por sua estrutura cíclica e modular.

Proposição 2.4. Todo grupo cíclico definido da forma dada anteriormente é gerado por $[1]_n \in \mathbb{Z}/n\mathbb{Z}$.

Demonstração. É fácil ver que $|[1]_n| = n$, assim como tal grupo possuí n elementos, e como todo $m[1]_n, 0 \leq m < n, m \in \mathbb{Z}$ são distintos dois a dois, $[1]_n$ gera esse grupo. □

Proposição 2.5. Da proposição anterior, vemos que a ordem de qualquer $[m]_n \in \mathbb{Z}/n\mathbb{Z}$ é $1, n|m$ e caso contrário:

$$|[m]_n| = \frac{n}{\gcd(m, n)}$$

Essa última proposição nos revela uma propriedade ainda mais importante desses grupos:

Corolário 2.1. A classe $[m]_n$ gera $\mathbb{Z}/n\mathbb{Z}$ se só se $\gcd(m, n) = 1$

Esse fato se torna ainda mais relevante, quando consideramos o caso em que $n = p$ tal qual p é primo, já que toda classe de equivalência não nula geraria esse grupo.

Temos ainda que, tomando $(\mathbb{Z}/n\mathbb{Z})^* := \{[m]_n \in \mathbb{Z}/n\mathbb{Z} | \gcd(m, n) = 1\}$ munido da operação de multiplicação $[a]_n, [b]_n \in (\mathbb{Z}/n\mathbb{Z})^*, [a]_n \cdot [b]_n = [a \cdot b]_n$ é um grupo.

Esse fato pode ser observado já que $\gcd(m_1, n) = \gcd(m_2, n) = 1 \implies \gcd(m_1 m_2, n) = 1$ (operação bem definida), cuja associatividade e identidade são resultados da multiplicação nos inteiros. Agora para observar a existência da inversa, vemos que como todo elemento desse grupo gera o grupo aditivo $\mathbb{Z}/n\mathbb{Z}$, então: $\exists a \in \mathbb{Z}, a \cdot [m]_n = [1]_n$