Universidade Federal do Rio de Janeiro
Instituto de Matemática

Notas em Algebra

Douglas Vieira
dvieira@disroot.org

10/2021

Conteúdo

Mapeamento

Vamos começar a entender o que é uma estrutura algébrica como introdução. Tome um conjunto S e incorpore esse conjunto com uma estrutura algébrica assumindo que nós podemos combinar, de várias formas (geralmente em duas), os elementos desse conjunto S para obter os elementos desse conjunto S. Isso que estamos fazendo aqui é combinar elementos do conjunto S, denominado de *operações em* S. Uma coisa importante para saber agora é que o comportamento dessas operações em S podem ser condicionadas impondo certos axiomas, alterando a natureza de S. Os axiomas definem a particularidade da estrutura em S. Se eu quiser pegar uma coleção de axiomas e testá-los na tentativa de definir novas estruturas seria algo possível. Repare nas palavras "testá-los"e "tentativa". Uma estrutura algébrica depende fortemente de **consistência** entre sua coleção de axiomas. Mesmo assim ainda não seria suficiente para evitar criar um sistema estranho. Daqui em diante trataremos os axiomas como regras que são validadas dentro de um sistema algébrico, não como verdades evidentes como é popularmente entendido.

Função Geral

Sendo S um conjunto de todos os objetos em venda num mercado e T ser o conjunto de todos os números reais. Definimos $f : S \to T$ como $f(s)$ = preço de s. Isso é um exemplo de mapeamento de S para T. Um exemplo de função: Sendo S um conjunto não vazio e definindo $i : S \to S$ como $i(s) = s$ para qualquer $s \in S$. Chamamos essa função, onde temos S para S, de função identidade.
Um mapeamento é uma função geral que associa um elemento de uma origem a um elemento **único** do destino. Chamaremos f como um mapeamento de S para T por $f : S \to T$ e, para $t \in T$, $t = f(s)$; t é *imagem* de s sob f. Assim, uma função é um mapa de um domínio D para um contradomínio CD tal que cada elemento de D tem pelo menos uma imagem em CD.

Definição 1. Se $g : S \to T$ e $f : T \to U$, então a *composição*, denotada por $f \circ g$, é o mapameanto $f \circ g : S \to U$ definido por $(f \circ g)(s) = f(g(s))$ para todo $s \in S$.

Lema 1. Se $h : S \to T$, $g : T \to U$ e $f : U \to V$, então $f \circ (g \circ h) = (f \circ g) \circ h$.

Demonstração. Temos que verificar que se esses dois mapeamento são iguais eles devem fazer a mesma coisa para qualquer elemento.
$\forall s \in S, (f \circ (g \circ h))(s) = ((f \circ g) \circ h)(s)$. A aplicação da definição de composição segue

$$(f \circ (g \circ h))(s) = f((g \circ h)(s)) = f(g(h(s)))$$

$$((f \circ g) \circ h)(s) = (f \circ g)(h(s)) = f(g(h(s))),$$

$$(f \circ (g \circ h))(s) = ((f \circ g) \circ h)(s), \forall s \in S.$$

Consequentemente, por definição, $f \circ (g \circ h) = (f \circ g) \circ h$. ∎

Funções Lineares

Uma das mais importantes classes de funções. Considere o conjunto

$$\mathbb{R}^n_m = \left\{ \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \mid a_{ij} \in \mathbb{R} \right\}.$$

Em particular, $\mathbb{R}^1_2$ é o conjunto dos vetores coluna bidimensionais

$$\hat{v} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}; v_1, v_2 \in \mathbb{R}.$$

Cada matriz real quadrada de ordem 2 resulta em uma função linear

$$L_A : \mathbb{R}^1_2 \to \mathbb{R}^1_2; \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \mapsto \begin{bmatrix} a_{11}v_1 + a_{12}v_2 \\ a_{21}v_1 + a_{22}v_2 \end{bmatrix}$$

ou

$$L_A(\hat{v}) = A\hat{v}.$$

Claro que

$$L_A \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} a_{11} \\ a_{21} \end{bmatrix} \quad \text{e} \quad L_A \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} a_{12} \\ a_{22} \end{bmatrix},$$

isto é, a função linear L_A determina a matriz A.
Seja B uma matriz quadrada de ordem 2 com uma função linear correspondente $L_B : \hat{v} \mapsto B\hat{v}$, BA é definida por

$$\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = \begin{bmatrix} b_{11}a_{11} + b_{12}a_{21} + b_{12}a_{22} \\ b_{21}a_{11} + b_{22}a_{21} + b_{22}a_{22} \end{bmatrix}.$$

A equação $L_{BA}(\hat{v}) = L_B \circ L_A(\hat{v})$ é verdadeira para todo $\hat{v}$ em $\mathbb{R}^1_2$.
A multiplicação de matrizes acompanha a composição das funções lineares correspondentes. Em particular, a associatividade da multiplicação de matriz é uma consequência direta da associatividade da composição de funções (**Lema** 1).

Semigrupos de Funções

Um mapa (ou função) $f : X \to X$ de X para ele mesmo é muitas vezes dito como um *autom-mapa* do conjunto X. Nesse contexto, o conjunto algumas vezes é chamado de *conjunto base* para a função $f : X \to X$.

Definição 2. Um conjunto S de funções $f : X \to X$ com o domínio X e contradomínio X é dito ser um semigrupo de funções no conjunto base X se

$$f \quad \text{e} \quad g \quad \text{em} \quad S \quad \text{implica} \quad g \circ f \quad \text{em} \quad S.$$

Nesse caso, S está fechado sob a composição (composta).
Se f é um elemento de um semigrupo S de funções, as exponenciais f^n para n inteiros positivos são definidas recursivamente por $f^1 = f$ e $f^{n+1} = f^n \circ f$.
Alguns exemplos de semigrupos de funções são:

Exemplo 1 (Auto-mapas)**.** Para um conjunto base X, defina X^X como o conjunto de todas as funções de X para X. Então X^X forma um semigrupo de funções em X.

Exemplo 2 (Funções constantes)**.** Seja X um conjunto e Y um subconjunto de X. Para cada elemento y de Y, define uma função constante

$$\begin{aligned} c_y : X &\to X \\ x &\mapsto y. \end{aligned}$$

Ainda temos que para cada elemento x de X, $y \in X$ e z no subconjunto Y

$$c_z \circ c_y(x) = c_z\left(c_y(x)\right) = c_z(y) = z = c_z(x),$$

ou seja, $c_z \circ c_y = c_z$. Assim o conjunto

$$C_Y = \left\{c_y \mid y \in Y\right\}$$

forma um semigrupo de funções em X.

Definição 3 (Função identidade)**.** Para qualquer conjunto X, a função identidade id_X é definida por

$$\begin{aligned} \mathrm{id}_X : X &\to X \\ x &\mapsto x. \end{aligned}$$

Para conjuntos X, Y e $f : X \to Y$, temos

$$\mathrm{id}_Y \circ f = f = f \circ \mathrm{id}_X.$$

Definição 4 (Monóide de Funções)**.** Um conjunto S de auto-mapas em um conjunto base X é dito ser um monóide de funções em X se formar um semigrupo e se a função identidade id_X é um elemento de S.

Um exemplo trivial de um monóide de função é o conjunto X^X em X.

Exemplo 3. Pelas funções lineares o conjunto $L(2, \mathbb{R})$ das funções lineares de $\mathbb{R}^1_2$ para ele mesmo forma um semigrupo de funções em $\mathbb{R}^1_2$. Agora para a matriz identidade

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

a função linear L_{I_2} é a função identidade $\mathrm{id}_{\mathbb{R}^1_2}$, então $L(2, \mathbb{R})$ forma um monóide de funções em $\mathbb{R}^1_2$.

Injetividade e sobrejetividade

Um mapeamento (a função f) $f : X \to Y$ precisa associar um unico valor da função $f(x)$ no contradomínio Y para cada argumento x do domínio X. Por outro lado, pode acontecer que argumento diferentes sejam associados ao mesmo valor $f(x)$. O caso trivial que serve de exemplo é a função dos quadrados $sq : \mathbb{Z} \to \mathbb{N}$ onde poderiamos ter

$$sq(-5) = (-5)^2 = 25 = 5^2 = sq(5).$$

Definição 5 (Função Injetiva)**.** Uma função $f : X \to Y$ é dita ser injetiva, ou *um para um*, se

$$f(x) = f(x') \implies x = x'$$

para todos elementos x e x′ do domínio S. Em essência, a equação $f(s) = t$ precisa ter uma única solução x em X para cada elemento y para a imagem de f. É imediato que qualquer função com um domínio vazio seja injetiva. Diferente da função $sq : \mathbb{Z} \to N$, a função $sqn : \mathbb{N} \to \mathbb{N}; n \mapsto n^2$ é injetiva.

Proposição 1 (Retração de funções injetivas)**.** Deixe $f : X \to Y$ injetiva, com o domínio não vazio. Então existe uma função

$$r : Y \to X$$

tal que

$$r \circ f = \mathrm{id}_X.$$

Demonstração. Escolha um elemento x_0 de X. Para um elemento y do contradomínio que não está na imagem $f(X)$, defina $r(y) = x_0$. Agora considere um elemento y da imagem de $f(X)$. Pela definição de imagem, a equação $f(x) = y$ tem um solução. Como f é injetiva, a solução é única.
Defina $r(y)$ como este único elemento de solução x_y.
Obtemos uma função $r : Y \to X$. Agora $r \circ f : X \to X$. Então para cada elemento x de X, temos

$$r \circ f(x) = r(f(x)) = x_{f(x)} = x = \mathrm{id}_X(x),$$

que verifica $r \circ f = \mathrm{id}_X$. ∎

Definição 6 (Retração)**.** Um mapeamento $r : Y \to X$ é cahamado de uma retração de uma função $f : X \to Y$ se $r \circ f = \mathrm{id}_X$.

Proposição 2 (Funções com retrações são injetivas)**.** Se uma função $f : X \to Y$ possui uma retração (volta), então ela é injetiva.

Demonstração. Deixe $r : Y \to X$ ser uma retração para f. Então

$$f(x) = f(x') \implies x = r \circ f(x) = r \circ f(x') = x'$$

para x, x' em X. ∎

A proprosição anterior mostra que cada injeção com domínio não vazio tem uma retração. Note que um injeção f pode ter muitas retrações, por causa da escolha arbitrária do elemento x_0 na prova da existência da retração. Também, note que a função identidade $id_\varnothing$ no conjunto vazio possui sua própria retração.

Definição 7 (Função Sobrejetiva)**.** Uma função $f : X \to Y$ é dita ser sobrejetiva se o contradomínio e imagem coincidem: $Y = f(X)$.

Maneiras para dizer que um mapeamento $f : X \to Y$ é sobrejetivo:

$$f(X) = \{f(x) \in Y \mid x \in X\}$$

$$f(X) = Y.$$

Ainda, a imagem inversa

$$f^{-1}\{y\} = \{x \in X \mid f(x) = y\}$$

necessita ser não vazia para cada elemento y de Y. Perceba que a única função sobrejetiva com um domínio vazio é a função identidade $id_\varnothing$ no conjunto vazio.
Um exemplo trivial de uma função sobrejetiva seria a função do valor absoluto $abs : \mathbb{Z} \to \mathbb{N}; n \mapsto |n|$

Proposição 3 (Seções de funções sobrejetivas)**.** Deixe $f : X \to Y$ ser sobrejetiva. Então existe uma função

$$s : Y \to X$$

tal que

$$f \circ s = id_y.$$

Definição 8 (Seções)**.** Uma função $s : Y \to X$ é chamada de seção de uma função $f : X \to Y$ se $f \circ s = id_Y$.

Proposição 4 (Funções com seções são sobrejetivas)**.** Se uma função $f : X \to Y$ tem uma seção, então ela é sobrejtiva.

Demonstração. Deixe $s : Y \to X$ ser uma seção para f. Então

$$f(s(y)) = f \circ s(y) = id_Y = y$$

para cada elemento y de Y. ∎

Cada sobrejeção tem uma seção. Note que uma sobrejeção f pode ter muitas seções.

Isomorfismo

Definição 9 (Isomorfismo de conjuntos)**.** A função $f : X \to Y$ é bijetivo se f é injetivo e sobrejetivo.

A utilização do mapeamento começa a se expandir quando entramos em composições de mapeamentos. Situa-se dois mapeamentos $g : X \to Y$ e $f : Y \to Z$. Queremos fazer com que os elementos de X sejam conduzidos ao conjunto Z. Com efeito, $g(x) \in Y$, sendo $f : Y \to Z$, tem-se a disponibilidade de $f(g(x)) \in Z$. Assim, $(f \circ g) : X \to Z$. Então, há o mapeamento de X para Z.

Lema 2. Se $f : X \to Y$ é uma bijeção, então $f \circ f^{-1} = id_Y$ e $f^{-1} \circ f = id_X$, onde id_X e id_Y são as identidades dos mapeamentos de X e de Y, respectivamente.

Demonstração. Primeiramente, temos $(f \circ f^{-1})(y) = f(f^{-1}(y))$. Pela definição, f^{-1} é o elemento $x_0 \in X$ tal que $y = f(x_0)$. Então $f(f^{-1}(y)) = f(x_0) = y$. Ora, isso significa que $(f \circ f^{-1})(y) = y$, validando a identidade deste mapeamento em Y. ■

Para $f^{-1} \circ f = id_X$ funciona analogamento como para id_Y

Definição 10. Para uma função $f : X \to Y$, uma função $g : Y \to X$ satisfazendo $g \circ f = id_x$ e $f \circ g = id_Y$ é chamado de inversa de f.

Se existe um isomorfismo $f : X \to Y$ de um conjunto X para um conjunto Y, podemos escrever

$$X \cong Y$$

e dizer que os conjunto X e Y são isomorfico. Nesse caso $Y \cong X$, em virtude do isomorfismo f^{-1}.
A ténica padrão para mostrar que dois conjuntos X e Y são isomorficos exibir duas funções mutuamente inversas $f : X \to Y$ e $g : Y \to X$.

Exemplo 4. Para cada númera natural n, considere o conjunto finito

$$N = \{0, 1, 2, ..., n - 1\}$$

dos números naturais menos do que n. Note que o conjunto N tem n elementos. Em particular, $\widehat{0}$ é o conjunto vazio. Agora, se um conjunto finito X tem n elementos, digamos $X = \{x_0, x_1, ..., x_{n-1}\}$, então existe uma bijeção

$$\begin{aligned} K : N &\to X \\ i &\mapsto x_i. \end{aligned}$$

De fato, um conjunto X tem n elementos se, e somente se existe uma bijeção $K : N \to X$. Nós podemos dizer que K *conta* os elemetnos de X. O número dos elemetnos em um conjunto finito X é chamado de *tamanho* ou *ordem* de X. É escrito como $| X |$. Dois conjunto são isomorficos se e somente se $| X | = | Y |$.

Grupos de permutações

Definição 11. Deixe X ser um conjunto.

(i.)

1. Uma função bijetiva $f : X \to X$ é chamada de uma permutação do conjunto X.
2. Um conjunto G de permutações em X é dito ser um grupo de permutações de X ou uma permutação no conjunto X se G é um monóide de funções satisfazendo a seguinte propriedade

$$f \in G \implies f^{-1} \in G$$

, também conhecida como *fechada sob a inversão*.

Equivalência

Ao estudarmos uma estrutura precisamos filtrar o que não é relevante para o estudo dela. A equivalência é este filtro. Um exemplo inicial de sua necessidade surge no conceito de número. O que significa o número 3? Um conjunto X tem 3 elementos se e somente se existe um isomorfismo de conjunto

$$f : \{1, 2, 3\} \to X$$

contando os elementos de X como $f(1), f(2)$ e $f(3)$. A função f tem que ser injetiva, de modo que nenhum elemento de X seja contado duas vezes. A função f tem que ser sobrejetiva, para garantir que cada elemento de X seja contado.
O único problema aqui é a circularidade. Para caracterizar o número 3, nós usamos esse número no domínio da função acima. Para escapar da circularidade nós podemos decidir considerar dois conjuntos como equivalentes para própositos de contagem sempre que eles forem isomórficos. O número 3 surge então como a propriedade que é comum a cada um dos conjuntos que são isomórficos a algum dado conjunto de 3 elementos (por exemplo $\{1,2,3\}$) ou $\{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}$). Os detalhes particulares dos elementos nos conjuntos não são relevantes para o problema da contagem, Eles são filtrados pela equivalência.

Núcleo e relações de equivalência

Considere a função dos quadrados $sq : \mathbb{Z} \to \mathbb{Z}; n \mapsto n^2$. Para dois inteiros n_1 e n_2,

$$sq(n_1) = sq(n_2) \quad \text{iff} \quad n_2 = \pm n_1.$$

Isto é, os inteiros n_1 e n_2 são associados ao mesmo valor de saída (valor da função) se e somente se ambos estão na mesma classe de equivalência $\{r, -r\}$. Essas classes de equivalência dividem o conjunto de domínios $\mathbb{Z}$ de inteiros, o que significa que $\mathbb{Z}$ se decompõe como a união

$$\mathbb{Z} = \{0\} \cup \{\pm 1\} \cup \{\pm 2\} \cup \{\pm 3\} \cup ...$$

de subconjuntos mutuamente disjuntos, as classes de equivalências.

Definição 12 (Relação de núcleo(kernel) de uma função)**.** Considere uma função $f : X \to Y$. Um par $\langle x1, x2\rangle$ de elementos de X é dito estar na relação de núcleo $\ker f$, denotada por $x1 \ker f x2$ ou por $x1(\ker f)x2$, se e somente se $x1$ e $x2$ são associados com a mesma saída (valor da função) por f. Formalmente

$$x1(\ker f)x2 \quad \text{iff} \quad f(x1) = f(x2).$$

A relação de núcleo $\ker f$ de uma função $f : X \to Y$ é reflexiva:

$$x(\ker f)x$$

para todo x em X. Também é transitiva:

$$(x_1(\ker f)x_2 \quad \text{e} \quad x_2(\ker f)x_3) \implies x_1(\ker f)x_3,$$

como $f(x_1) = f(x_2)$ e $f(x_2) = f(x_3)$ implica em $f(x_1) = f(x_3)$. E, por fim, também é simétrica:

$$x_1(\ker f)x_2 \implies x_2(\ker f)x_1.$$

Proposição 5 (Núcleos são relações de equivalência)**.** Deixe $f : X \to Y$ ser uma função. Então a relação de núcleo $\ker f$ de f é uma relação de equivalência no domínio X da função f.

Classes de equivalência

O kernel da função quadrática $sq : \mathbb{Z} \to \mathbb{Z}$ produziu a partição $\mathbb{Z} = \{0\} \cup \{\pm 1\} \cup \{\pm 2\} \cup \{\pm 3\} \cup ...$ de $\mathbb{Z}$. Temos que cada relação de equivalência em um conjunto produz uma partição do conjunto.

Definição 13. Se R é uma relação de equivalência em um conjunto X, define a classe de equivalência de x sob R sendo o conjunto

$$[x]_R = \{t \in X \mid xRt\}$$

de todos os elementos t de X que estão relacionados a x por R.

Pela reflexividade cada classe $[x]_R$ é não vazia porque contém pelo menos o próprio x. Pela relação kernel (ker f) de uma função $f : X \to Y$, e para um elemento x do domínio X, as classes de equivalência são dados pelos conjuntos de imagem inversa

$$[x]_{ker\ f} = f^{-1}\{f(x)\}.$$

Aqui está a propriedade chave de particionamento das relações de equivalência.

Proposição 6 (Classes de equivalência são disjuntas ou iguais)**.** Deixe R ser uma relação de equivalência no conjunto X. Deixe x_1 e x_2 serem elementos de X. Então as duas classes equivalência $[x_1]_R$, $[x_2]_R$ são ambas disjuntas:

$$[x_1]_R \cap [x_2]_R = \varnothing$$

ou iguais

$$[x_1]_R = [x_2]_R .$$

Em último caso, $x_1 R x_2$.

Demonstração. Suponha que $[x_1]_R$ e $[x_2]_R$ não são disjuntos. Assim, eles possuem um elemento x' em comum. Então $x_1 R x'$ e $x_2 R x'$ pela definição de classes de equivalência. Pela *simetria*, $x' R x_2$. Então $x_1 R x'$ e $x' R x_2$ implica em $x_1 R x_2$ pela *transitividade*.
Suponha que x'' é um elemento de $[x_1]_R$, então $x_1 R x''$. Então

$$x_2 R x_1 R x''$$

implica $x_2 R x''$ pela transitividade, assim x'' é um elemento de $[x_2]_R$. Similarmente, cada elemento de $[x_2]_R$ é um elemento de $[x_1]_R$. Segue que as duas classes $[x_1]_R$ e $[x_2]_R$ são iguais. ■

Concluindo, temos que cada relação de equivalência R no conjunto X é a relação kernel de uma função adequada com X como domínio. Deixe X_R denotar o conjunto

$$\{[x]_R \mid x \in X\}$$

de todas as classes de equivalência sob R. É muito importante observar que X_R é um conjunto de conjuntos. Os elementos C do conjunto X_R são conjuntos (as classes de equivalências). É importante este conceito final porque está presente em uma das principais dificuldades no entendimento da algebra. A hierarquia (elementos - conjuntos - conjuntos de conjuntos) deve ser compreendida o mais breve possível antes de chegarmos a uma abstração mais avançada.

Proposição 7. Deixe R ser uma relação de equivalência em um conjunto X.

(a) Existe uma função sobrejetiva

$$\pi R : X \to X_R;\ x \mapsto [x]_R .$$

(b) A relação de núcleo da função πR é o próprio R.

O primeiro Teorema de Isomorfismo para conjuntos

A função de divisão $\setminus : X \to \mathbb{R}; (n, m) \mapsto n^{-1}m$ (sendo a imagem dessa função o conjunto dos racionais) se decompõe como um composto da sobrejeção $X \to X_R$, o isomorfismo $X_R \cong \mathbb{Q}$, e a injeção $\mathbb{Q} \hookrightarrow \mathbb{R}$. O primeiro Teorema de Isomorfismo para conjuntos mostra que toda função pode ser escrita como uma composição

$$\langle \text{injeção} \rangle \circ \langle \text{isomorfismo} \rangle \circ \langle \text{sobrejeção} \rangle$$

Notação

$\hookrightarrow$ denota um monomorfismo, ou morfismo injetivo. Como $\mathbb{Q} \subset \mathbb{R}$, isto é, neste contexto, $\mathbb{Q}$ é uma subestrutura de $\mathbb{R}$, temos uma injeção natural, onde os elementos de $\mathbb{Q}$ são tratados como um elemento de $\mathbb{R}$.

Considere uma função $f : X \to Y$. Como a relação de núcleo $\ker f$ é uma relação de equivalência, a proposição (a) anterior mostra que existe uma função sobrejetiva

$$s : X \to X_{\ker f};\ x \mapsto [x]_{\ker f}.$$

Por outro lado, existe uma injeção

$$j : f(X) \hookrightarrow Y;\ y \mapsto y$$

inserindo a imagem $f(X)$ como um subconjunto no contradomínio Y. O ingrediente restante é um isomorfismo entre o conjunto $X_{\ker f}$ das classes de núcleo e a imagem $f(X)$.

Proposição 8. Deixe $f : X \to Y$ ser uma função. Então existe uma *bijeção bem definida*

$$b : X_{\ker f} \to f(X);\ [x]_{\ker f} \mapsto f(x).$$

Teorema 3 (Primeiro Teorema de Isomorfismo para conjuntos)**.** Deixe $f : X \to Y$ ser uma função. Então f se decompõe como a composta

$$f = j \circ b \circ s.$$

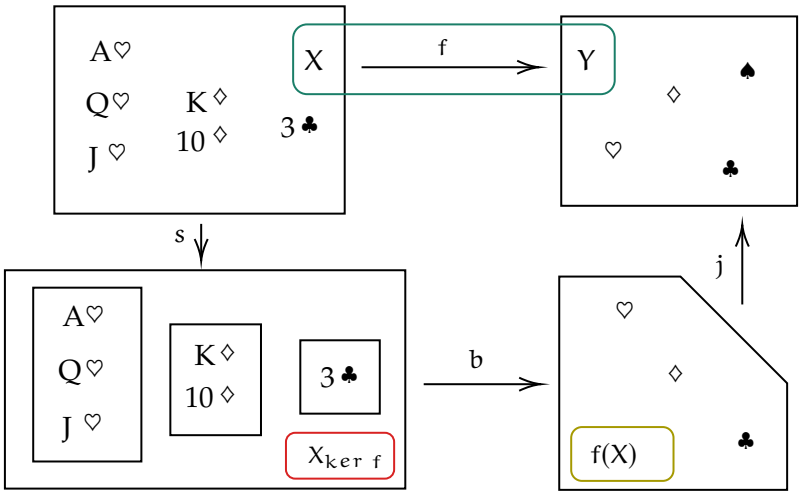

Ilustração do Primeiro Teorema de Isomorfismo.

O domínio X é o conjunto das cartas em mãos. O contradomínio Y é o conjunto completo de naipes. A função f mapeia cada carta na mão para o seu naipe, portanto duas cartas estão na relação $\ker f$ se e somente se eles estão no mesmo naipe. A classe de equivalência

$$[Q\heartsuit]_{\ker f} = \{J\heartsuit, Q\heartsuit, A\heartsuit\}$$

consiste de todas as copas na mão, a classe

$$[K\diamondsuit]_{\ker f} = \{10\diamondsuit, K\diamondsuit\}$$

consiste de todos os ouros na mão, e a classe $[3\clubsuit]_{\ker f}$ contém o único de paus na mão. A imagem

$$f(X) = \{\heartsuit, \diamondsuit, \clubsuit\}$$

é conjunto dos naipes que estão na mão. O primeiro teorema de isomorfismo exibe esse conjunto como isomórfico ao conjunto

$$X_{\ker f} = \{[Q\heartsuit]_{\ker f}, [K\diamondsuit]_{\ker f}, [3\clubsuit]_{\ker f}\}$$

das classes de equivalência. De fato, ambos $f(X)$ e $X_{\ker f}$ possuem 3 elementos cada. O fato de que os 3 elementos do conjunto $X_{\ker f}$ são conjuntos é irrelevante. Quando estamos lidando com conjuntos de classes de equivalência desconsidere os detalhes internos das classes por um momento, e apenas considere cada classe como um elemento.

Grupos e Monóides

Se S é um semigrupo de funções, então podemos considerar a função composta como um mapa

$$S \times S \to S$$
$$(g, f) \mapsto g \circ f.$$

cujo domínio é o conjunto $S \times S$ dos pares ordenados (g, f) dos elementos de S. Estar fechado sob a composição, isto é, $g \in S$ e $f \in S$ implica implica $g \circ f \in S$, garente que S pode servir como o contradomínio do mapa acima.
Lembrando que a função composta é sempre associativa. As propriedades abstratas dos semigrupos de funções são revisadas na definição seguinte.

Definição 14 (Semigrupos)**.** Deixe S ser um conjunto equipado com um mapa

$$S \times S \to S$$
$$(x, y) \mapsto g * f$$

associando um elemento $x * y$ ou xy de S a cada par ordenado (x, y) dos elementos de S.

(a) Em geral, o mapa anterior é conhecido como uma multiplicação S ou (formalmente) como uma operação binária em S.

(b) A existência de tal mapa é descrita como o fechamento do conjunto S com respeito a multiplicação.

(c) O par $(S, *)$ consistindo do conjunto S com a operação $*$ é chamado de *semigrupo* (ou *semigrupo abstrato*) se a lei associativa

$$x * (y * z) = (x * y) * z$$

é válida para todos elementos x, y e z do conjunto S.

Definição 15 (Comutatividade)**.** Dois elementos x e y de um semigrupo $(S, *)$ são ditos que comutam se $x * y = y * x$. O semigrupo $(S, *)$ é dito ser comutativo se $x * y = y * x$ para todo x,y em S.

Exemplo 5. Deixe S ser o conjunto ou o intervalo $(1, \infty)$ dos números reais x com $x > 1$. Então S forma um semigrupo sob a multiplicação usual (associativa e comutativa) dos números reais.

Exemplo 6. Considere o conjunto dos inteiro $\mathbb{Z}$. Então $\mathbb{Z}$ é fechado sob a operação de subtração

$$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$
$$(x, y) \mapsto x - y.$$

No entanto, $\mathbb{Z}$ não forma um semigrupo sob a subtração, pois a subtração não é associativa. De fato,

$$3 - (5 - 4) = 3 - 1 = 2,$$

enquanto

$$(3 - 5) - 4 = (-2) - 4 = -6.$$

Monóides

Um monóide de funções em um conjunto X é um semigrupo de funções em X que contém a função identidade id_X em X.

Definição 16 (Monóides abstratos)**.** Deixe $(M, *)$ ser um semigrupo com $*$ como operação. Então M é dito formar um *monóide* (ou um *monóide abstrato*) $(M, *, e)$ se ele contém um elemento e satisfazendo

$$e * x = x = x * e$$

para todo x em M. O elemento e é conhecido como o elemento identidade do monóide M.

Exemplo 7. O semigrupo $S = (1, \infty)$ do exemplo anterior não forma um monóide. Certamente S não contém o elemento identidade 1 para a multiplicação dos números reais. De fato, para cada elemento e de S, nós temos $e * x > x$ para todo x em S. Assim nenhum elemento e (não há nenhum elemento identidade, pois, pela proposição a seguir veremos que o elemento e é único) de S pode satisfazer a definição de monóide abstrato.

Proposição 9 (Unicidade do elemento identidade)**.** Deixe M ser um monóide. Se e e f são elementos identidade de M, então $e = f$. Assim o elemento identidade de um monóide é único.

Demonstração. Temos $e = e * f = f$. A primeira igualdade é válida pois f é um elemento identidade. A segunda igualdade é válida pois e é um elemento identidade. ■

Grupos

Definição 17 (Grupos Abstratos)**.** Um monóide $(G, *, e)$ é um *grupo* (ou um *grupo abstrato*) se cada elemento x de G tem um inverso x^{-1} em G com

$$x * x^{-1} = e = x^{-1} * x.$$

Ou seja, um grupo $(G, *, e)$ é um conjunto G com uma multiplicação $*$ satisfazendo as seguintes propriedades

- **Fechado:** $x * y \in G, \forall x, y \in G$;
- **Associatividade:** $x * (y * z) = (x * y) * z, \forall x, y, z \in G$;
- **Identidade:** $\exists e \in G; e * x = x = x * e, \forall x \in G$;
- **Inverso:** Para cada x em G existe x^{-1} em G com $x * x^{-1} = e = x^{-1} * x$.

Grupos comutativos também são chamados de abelianos.

Em essência,
Semigrupos precisam satisfazer as propriedades fechado e associatividade;
Monóides precisam satisfazer as propriedades fechado, associatividade e identidade;
Grupos precisamos satisfazer as propriedades fechado, associatividade, identidade e inverso.

Proposição 10 (Unicidade dos inversos)**.** Em um grupo G, cada elemento x tem um único inverso.

Exemplo 8. Os números reais formam um grupo $(\mathbb{R}, +, 0)$ com a adição sendo a operação comutativa. O inverso ou inverso aditivo do número real r é $-r$. $(\mathbb{R}, +, 0)$ é um grupo aditivo onde o elemento identidade (ou elemento neutro) é o 0 e o inverso é a negação de um elemento de $\mathbb{R}$.

Exemplo 9. Sob a multiplicação, os números reais diferentes de zero formam um grupo comutativo $(\mathbb{R}^*, \cdot, 1)$.

Definição 18 (Elementos inversíveis)**.** Deixe $(M, *, e)$ ser um monóide. Um elemento a de M é dito ser um inversível ou uma unidade se existe um elemento b de M tal que $a \cdot b = e = b \cdot a$.

Proposição 11 (Elementos inversíveis formam um grupo)**.** Deixe $(M, *, e)$ ser um monóide. Então o conjunto M^* dos elementos inversíveis de M forma um grupo $(M^*, *, e)$.

Definição 19 (O grupo de unidades)**.** Para um monóide $(M, *, 1)$, o grupo $(M^*, *, 1)$ é conhecido como o grupo de unidades do monóide M.

Exemplo 10. Os inteiros formam um monóide comutativo $(\mathbb{Z}, \cdot, 1)$ sob a multiplicação. O grupo de unidades do monóide de inteiros é $\{\pm 1\}$.

Exemplo 11. A notação da definição anterior (M^*) é consistente com o Exemplo 9: o conjunto de unidades do monóide dos números reais sob a multiplicação é o conjunto $\mathbb{R}^*$.

Estrutura dos componentes

Existem métodos para obtermos novos semigrupos, monóides ou grupos a partir dos que foram dados. Um dos métodos é a construção do produto direto. Relembre que para conjuntos X e Y, o *produto direto* (externo) ou *produto* de X e Y é o conjunto

$$X \times Y = \{(x, y) \mid x \in X, y \in Y\}$$

dos pares ordenados (x, y) dos elementos x de X e y de Y. Nesse contexto, os conjuntos X e Y são conhecidos como *fatores* (direto) do produto direto. O conjunto $X \times Y$ é chamado de produto cartesiano de X e Y. Lembrando que dois pares ordenados (x, y) e (x', y') são iguais se e somente se $x = x'$ e $y = y'$. Escrevemos X^2 para $X \times X$, descrevendo-o como o *quadrado direto* do conjunto X.
Suponha que X é um semigrupo sob a multiplicação $\circ_X$, enquanto Y é um semigrupo sob a multiplicação $\circ_Y$. Nós podemos então definir a multiplicação em $X \times Y$ por

$$(x_1, y_1) \circ_{X\times Y} (x_2, y_2) = (x_1 \circ_X x_2, y_1 \circ_Y y_2)$$

para x_1, x_2 em X e y_1, y_2 em Y. A multiplicação acima é descrita como um *componente de multiplicação*, pois funciona individualmente nos componentes x e y dos pares ordenados.

Proposição 12 (Produto direto de semigrupos)**.** Deixe $(X, \circ_X)$ e $(Y, \circ_Y)$ serem semigrupos. Então sob a componente de multiplicação definida acima, o produto direto $X \times Y$ forma um semigrupo.

Definição 20. O semigrupo $(X\times Y, \circ_{X\times Y})$ da proposição anterior é chamado de produto direto (externo) dos semigrupos $(X, \circ_X)$ e $(Y, \circ_Y)$.

Exemplo 12 (O plano real)**.** O conjunto $\mathbb{R}$ dos números reais forma um semigrupo sob a multiplicação. Então o plano real $\mathbb{R}^2$ forma um semigrupo sob a componente de multiplicação.

Se os semigrupos $(X, \circ_X)$ e $(Y, \circ_Y)$ são monóides, com respeito ao elemento identidade e_X e e_Y, então o *componente do elemento identidade* é o elemento

$$e_{X\times Y} = (e_X, e_Y)$$

de $X \times Y$.

Proposição 13. Deixe $(X, \circ_X, e_X)$ e $(Y, \circ_Y, e_Y)$ serem monóides. Então sob a componente de multiplicação, o produto direto $X \times Y$ forma um monóide

$$(X \times Y, \circ_{X\times Y}, e_{X\times Y})$$

com a componente do elemento identidade.

Definição 21 (O produto direto de dois monóides)**.** O monóide $(X \times Y, \circ_{X\times Y}, e_{X\times Y})$ da proposição anterior é chamado de produto (externo) direto dos dois monóides $(X, \circ_X, e_X)$ e $(Y, \circ_Y, e_Y)$.

A etapa final do estudo da estrutura dos componentes considera os grupos. Suponha que $(X, \circ_X, e_X)$ e $(Y, \circ_Y, e_Y)$ são grupos. Então, para um elemento (x, y) de $X \times Y$, defina o *componente inverso*

$$(x, y)^{-1} = (x^{-1}, y^{-1})$$

como um elemento de $X \times Y$.

Proposição 14. Deixe $(X, \circ_X, e_X)$ e $(Y, \circ_Y, e_Y)$ serem grupos. Então o produto direto $X \times Y$ forma um grupo

$$(X \times Y, \circ_{X\times Y}, e_{X\times Y})$$

sob a componente de multiplicação, componente do elemento identidade e sob componente inverso.

Definição 22 (O produto direto de dois grupos)**.** O grupo

$$(X \times Y, \circ_{X\times Y}, e_{X\times Y})$$

da proposição anterior é chamado de produto (externo) direto dos dois grupos $(X, \circ_X, e_X)$ e $(Y, \circ_Y, e_Y)$.

Exemplo 13. O conjutno $\mathbb{R}$ dos números reais forma um grupo sob a operação de adição. Então o plano real $\mathbb{R}^2$ forma um grupo sob a componente de adição:

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2).$$

Observe bem: esta é a adição trivial de dois vetores reais em dimensão 2.

Teorema 4 (Grupos de unidades de produtos)**.** Deixe $(M_1, *, e_1)$ e $(M_2, *, e_2)$ são monóides. Então o grupo das unidades $(M_1 \times M_2)^*$ do produto de monóide $M_1 \times M_2$ é o produto $M_1^* \times M_2^*$ dos grupos de unidades M_1^*, M_2^* dos repectivos fatores M_1, M_2.

É relativamente fácil expandir as contruções de produto para um grande número de fatores. Por exemplo, um produto $X \times Y \times Z$ dos conjuntos X, Y e Z pode ser construído recursivamente como $X \times (Y \times Z)$, ou diretamente como o conjunto

$$X \times Y \times Z = \{(x, y, z) \mid x \in X, y \in Y, z \in Z\}$$

de triplas ordenadas. O produto $X \times X \times X$ é conhecido como o cube (direto) X^3 do conjunto X.
Por exemplo, o cubo direto $\mathbb{R}^3$ do grupo aditivo $(\mathbb{R}, +, 0)$ dos números reais, com a estrutura de componente, é o grupo dos vetores de dimensão 3.
Um outro exemplo um pouco não trivial é o conjunto $\mathbb{R}_2^2$ das matrizes reais quadradas de ordem 2 carregando uma estrutura de componente aditivo de grupo com a adição dada pela adição usual:

$$\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} + \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = \begin{bmatrix} b_{11} + a_{11} & b_{12} + a_{12} \\ b_{21} + a_{21} & b_{22} + a_{22} \end{bmatrix}$$

O mesmo conjunto carrega uma estrutura de componente de monóide, com a multiplicação dada pela componente de multiplicação

$$\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \circ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = \begin{bmatrix} b_{11}a_{11} & b_{12}a_{12} \\ b_{21}a_{21} & b_{22}a_{22} \end{bmatrix}$$

das matrizes. Repare que esta não é a multiplicação trivial de matrizes. Esse produto de matrizes se chama *produto de Hadamard*.

Potências

Outra fonto de estrutura de componentes é achado nos conjuntos de funções $f : X \to S$ de um certo domínio X para um contradomínio S que carrega uma estrutura algebrica. Por exemplo, em cálculo a componente soma $f + g$ de duas funções reais $f : \mathbb{R} \to \mathbb{R}$ e $g : \mathbb{R} \to \mathbb{R}$ é determinada pela especificação

$$(f + g)(x) = f(x) + g(x)$$

para todo x em $\mathbb{R}$. Sob essa operação, o conjunto $\mathbb{R}^{\mathbb{R}}$ de todas as funções reais forma um grupo aditivo, com a função constante zero como o zero (elemento identidade), e a inversa da função f dada pela negação $-f$, teremos

$$(-f)(x) = -f(x)$$

para todo real x.

Definição 23 (Estrutura das potências)**.** Deixe X e S serem conjuntos. Considere o conjunto S^X de todas as funções $f : X \to S$ de X para S.

(a) Se S carrega uma estrutura de semigrupo $(S, *)$, então o X-ésima potência $(S, *)^X$ ou S^X do semigrupo $(S, *)$ é o conjunto S^X equipado com a componente de multiplicação $f \cdot g$ dada por

$$(f \cdot g)(x) = f(x) \cdot g(x),$$

$\forall x \in X$.

(b) Se S carrega uma estrutura de monóide $(S, *, e_S)$, então o X-ésima potência $(S, *, e_S)^X$ ou S^X do monóide $(S, *, e_S)$ é o X é-simo potência do semigrupo $(S^X, *)$, com a função constante $E : X \to S;\ x \mapsto e_S$ como a componente do elemento identidade.

(c) Se S carrega uma estrutura de grupo $(S, *, e_S)$, então o X-ésima potência $(S, *, e_S)^X$ ou S^X do grupo $(S, *, e_S)$ é o X é-simo expoento do monóide $(S^X, *, E)$, com a componente inversa da função $f : X \to S$ dada por $f^{-1}(x) = f(x)^{-1}$ para cada x em X.

Se X é o n-ésimo elemento conjunto $N = \{0, 1, ..., n-1\}$ para um inteiro positivo n, então as potências S^N são conhecidas como as n-ésimas potências S^n.

Exemplo 14 (Vetores)**.** Deixe n ser um inteiro positivo. Um vetor de n componentes (ou vetor de dimensão n) real é um elemento

$$(x_0, x_1, ..., x_{n-1})$$

do grupo de potência $\mathbb{R}^n$. Por exemplo, na Relatividade Especial um vetor de dimensão 4

$$(ct, x_1, x_2, x_3)$$

representa um evento no tempo t e a localização espacial (x_1, x_2, x_3) em um determinado referencial, c sendo a velocidade da luz.

Submonóide e Subgrupos

A estrutura de componente em produto de conjuntos é uma rica fonte de novos semigrupos, monóides e grupos. Uma outra é achada dos subconjuntos que são fechados sob uma dada estrutura.

Definição 24 (Subsemigrupos)**.** Deixe S, ou seja, $(S, *)$, ser um semigrupo, e deixe X ser um subconjunto de S. Então X é descrito como um subsemigrupo do semigrupo $(S, *)$ se ele satisfazer a propriedade *Fechado*:

$$x, y \in X \implies x * y \in X.$$

A associatividade de $(X, *)$ é um caso especial do próprio semigrupo que X herda (neste caso, o do semigrupo $(S, *)$). É imediato que o conjunto vazio é um subsemigrupo de todo semigrupo.

Exemplo 15 (Subsemigrupos dos inteiros sob a operação de adição)**.** O conjunto dos inteiros negativos forma um subsemigrupo do semigrupo $(\mathbb{Z}, +)$ dos inteiros sob a operação de adição. O conjunto dos inteiros ímpares não forma um subsemigrupo, pois a propriedade fechado é violada, por exemplo, por $1 + 3$.

Definição 25 (Submonóides)**.** Um subconjunto X de um monóide $(M, *, e)$ é dito ser um *submonóide* se ele é um subsemigrupo do semigrupo $(M, *)$, e se ele contém o elemento identidade e de M.

Se $(X, *, e)$ é um submonóide de um monóide $(M, *, e)$, então $(X, *, e)$ é um monóide: A propriedade de identidade para X é apenas um caso especial da propriedade de identidade para M. Trivialmente, o conjunto $\{e\}$ consistindo apenas do elemento identidade é um submonóide de qualquer monóide $(M, *, e)$ com e como elemento identidade.
Note que $\{e\}$ é um subsemigrupo pela propriedade de identidade: $e * e = e$.

Exemplo 16 (Submonóides de inteiros sob a operação de adição)**.** O subsemigrupo de inteiros negativos não forma um submonóide do monóide $(\mathbb{Z}, +, 0)$ de inteiros sob a adição, pois ele não contém o elemento identidade 0 de $\mathbb{Z}$. Por outro lado, o monóide $(\mathbb{N}, +, 0)$ dos números natural sob a adição forma um submonóide de $(\mathbb{Z}, +, 0)$.

Exemplo 17 (Matrizes Estocásticas)**.** Uma matriz real quadrada de ordem 2

$$A = \begin{bmatrix} p_1 & p_2 \\ q_1 & q_2 \end{bmatrix}$$

é dita ser (linha) estocástica se p_1, p_2, q_1, q_2 não são negativos,

$$p_1 + p_2 = 1, \quad \text{e} \quad q_1 + q_2 = 1.$$

Note que a matriz identidade I_2 é estocástica. Deixe Π_2^2 ser o conjunto das matrizes estocásticas. Então Π_2^2 forma um submonóide do monóide $\mathbb{R}_2^2$ de todas as matrizes quadradas de ordem 2 sob a multiplicação de matrizes.

Definição 26 (Subgrupos)**.** Um submonóide X de um grupo $(G, *, e)$ é dito ser um subgrupo de G se ele é fechado sob a inversão em G:

$$x \in X \implies x^{-1} \in X.$$

Note que o conjunto $\{e\}$ consistindo apenas do elemento identidade é um subgrupo de qualquer grupo $(G, *, e)$ com e sendo seu elemento identidade. Como um subgrupo tem que ser um submonóide, com um elemento identidade, ele também tem que ser não vazio. Existe uma maneira rápida de checar se um dado subconjunto não vazio X de um grupo G forma um subgrupo de G.
Veremos isso na proposição seguinte.

Proposição 15 (O teste do subgrupo)**.** Deixe X ser um subconjunto não vazio de um grupo $(G, *, e)$. Então X é um subgrupo de G se e somente se ele satisfaz a propriedade Fechado

$$x, y \in X \implies x * y^{-1} \in X.$$

Demonstração. Primeiro, suponha que X é um subgrupo de G, e que x e y são elementos de X. Então, pela propriedade de fechado na definiçao de subgrupo, y^{-1} está em X. Como x e y^{-1} está em X, a propriedade de fechamento (na definição de semigrupos) garante que $x * y^{-1}$ está em X.
Por outro lado, suponha que o subconjunto X do grupo G satisfaça a propriedade da proposição anterior (fechado). Como X não é vazio, contém um elemento a. Então a proriedade mostra que o elemento identidade $e = a * a^{-1}$ está em X. Denovo, para cada elemento x de X, a propriedade da proposição anterior mostra que a inversa $x^{-1} = e * x^{-1}$ está em X. Finalmente, para x e y em X, a propriedade mostra que o produto $x * y = x * (y^{-1})^{-1}$ está em X, então X forma um subsemigrupo de $(G, *)$. ■

Teorema 5 (Subgrupos de inteiros)**.** Deixe J ser um subgrupo do grupo $(\mathbb{Z}, +, 0)$ de inteiros sob a adição. Então existe um número natural d tal que J consiste do conjunto $d\mathbb{Z}$ de múltiplos inteiros de d.

Coclasse (Cosets)

Um semigrupo $(G, *)$ carrega uma operação associativa de seus elementos. É muito útil extendermos essa operação para subconjuntos de G.
Deixe X ser um subconjunto de um semigrupo $(G, *)$. Se g é um elemento de G, define-se

$$Xg = \{xg \mid x \in X\} \quad \text{e} \quad gX = \{gx \mid x \in X\}.$$

Esses conjuntos acima são conhecidos, respectivamente, como *coclasse à direita* e *coclasse à esquerda* do subconjunto X com o elemento g. Por exemplo, o subgrupo $d\mathbb{Z}$ do grupo $(\mathbb{Z}, +, 0)$ é a coclasse de d no semigrupo $(\mathbb{Z}, \cdot)$.
A notação é extendida pela configuração XY ou

$$X \cdot Y = \{x \cdot y \mid x \in X, y \in Y\}$$

para subconjuntos X e Y de um semigrupo $(G, \cdot)$. Em particular, $Xg = X \cdot \{g\}$ e $\{g\} \cdot X = gX$ para um elemento g de G.
Se X é um subconjunto de um monóide G com o elemento identidade e, então as coclasses eX e Xe coincidem com o subconjunto X.

Proposição 16 (Coclasses de grupo são isomórficos como conjuntos)**.** Deixe X ser um subconjunto de um grupo G. Então para elementos g_1, g_2 de G, as coclasses Xg_1, Xg_2 e g_1X são todos isomórficos como conjuntos.

Demonstração. Os mapas

$$\begin{aligned} X &\to Xg_1 \\ x &\mapsto xg_1 \end{aligned}$$

e

$$\begin{aligned} Xg_1 &\to X \\ y &\mapsto yg_1^{-1} \end{aligned}$$

são mutuamente bijeções inversas, então $X \cong Xg_1$. Lembre que isomorfismo é uma relação de equivalência. Segue que Xg_1 e Xg_2 são isomórficos. Similarmente, os mapas

$$\begin{aligned} X &\to g_1X \\ x &\mapsto g_1x \end{aligned}$$

e

$$\begin{aligned} g_1X &\to X \\ y &\mapsto g_1^{-1}y \end{aligned}$$

são mutuamente bijeções inversas, então $X \cong g_1X$. O resto da proposição segue do fato que isomorfismo é uma relação de equivalência. ■

Como dois conjuntos finitos são isomorficos se e somente se eles possuem o mesmo número de elementos, nós temos a seguinte consequência:

Corolário 5.1 (Coclasses finitas são todas do mesmo tamanho)**.** Deixe X ser um subconjunto finito de um grupo G. Então para os elementos g_1, g_2 de G, as cloclasses Xg_1, Xg_2 e g_1X possuem o mesmo número de elementos.

Observação

Coclasses de subgrupos são classes de equivalência.

Proposição 17. Deixe H ser um subgrupo de um grupo G.

a. Define-se uma relação R em G por

$$g_1Rg_2 \quad \text{iff} \quad hg_1 = g_2 \quad \text{for some} \quad h \in H.$$

Então R é uma relação de equivalência em G.

b. As classes de equivalência para R são as coclasses à direita Hg.

Teorema 6 (Teorema de Lagrange)**.** Deixe H ser um subgrupo de um grupo finite G. Então o número $| H |$ de elementos de H divide o número $| G |$ de elementos de G.

Demonstração. Pela proposição 17 e pela proposição 6, duas coclasses distintas de H são disjuntas. Suponha que existam j coclasses à direita ao todo. Pelo colorário anterior cada coclasse à direita tem $| H |$ elementos. Então

$$| G | = j \, | H |,$$

então $| H |$ divide $| G |$. ■

O número j =| G | /| H | é chamado de *índice* de H no grupo G. Geralmente, se G é um grupo infinito com um subgrupo H, o indice de H é o número (possivelmente infinito) de coclasses à direita de H em G.
O Teorema de Lagrange é útil para limitar os possíveis subgrupos de um dado grupo finito.
Em qualquer grupo G com o elemento identidade e, o subgrupo G é descrito como impróprio, enquanto o menor subgrupo $\{e\}$ é descrito como trivial. Um subgrupo H é próprio se ele não for impróprio. Como primos são números irredutíveis, o teorema de lagranre produz o seguinte resultado.

Proposição 18 (Grupos de ordem primo)**.** Um grupo com um número primo de elementos não pode ter subgrupos próprios e não triviais.

Proposição 19 (Cancelação em grupos)**.** Deixe G ser um grupo, com elementos x, y_1, y_2.
Se $x \cdot y_1 = x \cdot y_2$, então $y_1 = y_2$.
Se $y_1 \cdot x = y_2 \cdot x$, então $y_1 = y_2$.

Corolário 6.1 (Existência e unicidade de soluções)**.** Considere a equação

$$x * y = z$$

em um grupo $(G, *)$. Se a equação acima é válida, o conhecimento de qualquer dois elementos de x, y, z especifica o terceiro unicamente.

Homomorfismo

Um estudo de conjuntos inevitavelmente cai para um estudo de funções entre conjuntos. Similarmente acontece quando estudamos estruturas algébricas como semigrupos, monóides ou grupos, inevitavelmente estudamos as funções que preservam a estrutura algébrica. Essas funções são conhecidas como Homomorfismo.

Homomorfismo

Considere a função exponencial

$$\begin{aligned} &\mathbb{R} \to \mathbb{R} \\ &x \mapsto\ e^x. \end{aligned}$$

Pela regra dos expoentes,

$$E(x + y) = e^{x+y} = e^x \cdot e^y = E(x) \cdot E(y). \tag{1}$$

Aqui, o domínio da função exponencial E é o semigrupo $(\mathbb{R}, +)$ dos números reais sob a operação de adição. O contradomínio da função E é o semigrupo $(\mathbb{R}, \cdot)$ dos números reais sob a operação de multiplicação.
A equação (1) diz que podemos adicionar dois números reais x e y no domínio e então mapear para $E(x + y)$ no contradomínio, ou então mapear x e y individualmente para $E(x)$, $E(y)$ no contradomínio e multiplicá-los no contradomínio. Obtemos a mesma resposta com as duas formas.

> **Definição 27** (Homomorfismo de semigrupos, monóide e grupos)**.** Homomorfismo e isomorfismo.

i. Deixe $\phi : (X, \circ) \to (Y, *)$ ser uma função de um semigrupo $(X, \circ)$ para um semigrupo $(Y, *)$. Então ϕ é dito ser um *homomorfismo de semigrupo* se

$$\phi(x_1 \circ x_2) = \phi(x_1) * \phi(x_2)$$

$\forall x_1, x_2 \in X$.

ii. Deixe $\phi : (X, \circ, e) \to (Y, *, f)$ ser uma função de um monóide $(X, \circ, e)$ para um monóide $(Y, *, f)$. Então ϕ é dito ser um *homomorfismo de monóide* se ϕ for um homomorfismo de semigrupo $\phi : (X, \circ) \to (Y, *)$ com $\phi(e) = f$.

iii. Deixe $\phi : (X, \circ, e) \to (Y, *, f)$ ser uma função de um grupo $(X, \circ, e)$ para um grupo $(Y, *, f)$. Então ϕ é dito ser um *homomorfismo de grupo* se ϕ é um homomorfismo de monóide $\phi : (X, \circ, e) \to (Y, *, f)$ com $\phi(x^{-1}) = (\phi(x))^{-1}, \forall x \in X$.

iv. Bijeção de homomorfismo de semigrupo, monóide e grupo são descritos respectivamente como isomorfismo de semigrupo, monóide e grupo.

A relação de isomorfismo entre semigrupos, monóides ou grupos X e Y é frequentemente denotada por

$$X \cong Y$$

. O contexto aqui é o isomorfismo de conjuntos, semigrupos, monóides ou grupos.

Exemplo 18. A regra dos expoentes mostra que $E : (\mathbb{R}, +) \to (\mathbb{R}, \cdot)$ é um homomorfismo de semigrupo do semigrupo dos números reais sob a operação de adição para o semigrupo dos números reais sob a operação de multiplicação. Ainda

$$E(0) = 1$$

mostra que $E : (\mathbb{R}, +, 0) \to (\mathbb{R}, \cdot, 1)$ é um homomorfismo de monóide de um monóide dos números reais sob a operação de adição para o monóide dos números reais sob a operação de multiplicação.

Exemplo 19 (Inclusão de um subgrupo)**.** Deixe H ser um subgrupo de um grupo G. Então a função de inclusão

$$\begin{aligned} H &\hookrightarrow G \\ h &\mapsto h. \end{aligned}$$

é um homomorfismo de grupo.

Exemplo 20. Dados conjuntos X e Y, define-se respectivas projeções

$$\pi_1 : X \times Y \to X;\ (x, y) \mapsto x$$

e

$$\pi_2 : X \times Y \to Y;\ (x, y) \mapsto y$$

para o primeiro e o segundo fator. Se X e Y são semigrupos, monóides ou grupos então as projeções são homomorfismos de semigrupos, monóides, e grupo recpetivamente.

Proposição 20 (Homomorfismo de semigrupo entre grupos)**.** Deixe $\phi : (X, \circ) \to (Y, *)$ ser um homomorfismo de semigrupo entre dois grupos $(X, \circ, e)$ e $(Y, *, f)$. Então ϕ é um homomorfismo de grupo.

Demonstração. Como ϕ é um homomorfismo de semigrupo, a equação

$$\phi(e) * \phi(e) = \phi(e \circ e) = \phi(e)$$

é válida em Y. No entanto, como f é o elemento identidade de Y, e $\phi(e)$ é um elemento de Y, a propriedade de identidade em Y da

$$\phi(e) * f = \phi(e).$$

Segue que $\phi(e) * \phi(e) = \phi(e) * f$, então $\phi(e) = f$ pelo Corolário 6.1, e ϕ é um homomorfismo de monóide.
Agora para cada elemento x de X, nós temos

$$\phi(x) * \phi(x^{-1}) = \phi(x \circ x^{-1}) = \phi(e) = f.$$

Mas $\phi(x) * (\phi(x))^{-1} = f$, então pelo Corolário 6.1 novamente da $\phi(x^{-1}) = (\phi(x))^{-1}$, fazendo ϕ um homomorfismo de grupo. ∎

Teorema 7 (Homomorfismo de monóide e grupo de unidades)**.** Deixe $\phi : (M, \circ, e) \to (N, *, f)$ ser um homomorfismo de monóide. Então ϕ é restringido a um homomorfismo de grupo $\phi^* : M^* \to N^*$ entre grupos correspondentes de unidades.

Demonstração. Suponha que a está em M^*, com $a \circ b = e = b \circ a$ para algum $b em M$. Então

$$\phi(a) * \phi(b) = \phi(a \circ b) = \phi(e) = f = \phi(b) * \phi(a),$$

então $\phi(a)$ está em N^*. A restrição

$$\phi^* : M^* \to N^*;\ a \mapsto \phi(a)$$

é um homomorfismo de semigrupo entre os respectivos grupos de unidades. Pela Proposição anterior isso significa que se trata de um homomorfismo de grupo. ■

Uma função $f : X \to Y$ entre conjuntos é totalmente descrita pelo seu gráfico, o subconjunto

$$\{(x, f(x) \mid x \in X)\}$$

de $X \times Y$. Homomorfismos podem então serem reconhecidos pelos seus gráficos.

Proposição 21 (O gráfico de um homomorfismo)**.** Deixe $(X.\circ)$ e $(Y, *)$ serem semigrupos. Então uma função $f : X \to Y$ é um homomorfismo de semigrupo se e somente se o gráfico é um subsemigrupo do produto direto de semigrupo $X \times Y$.

Corolário 7.1. Deixe $(X, \circ, e)$ e $(Y, *, f)$ serem monóides. Então uma função $f : X \to Y$ é dita ser um homomorfismo de monóide se e somente se o gráfico ser um submonóide do produto direto de monóide $X \times Y$.

Subgrupo Normal

Deixe $f : X \to Y$ ser uma função. A imagem $f(X) = \{f(x) \mid x \in X\}$ é um subconjunto do contradomínio Y. Se f é um homomorfismo de semigrupos, monóides ou de grupos, a imagem irá carregar a correspondente estrutura algebrica.

Proposição 22 (Imagens de homomorfismos)**.** Deixe $f : (X, *) \to (Y, *)$ ser um homomorfismo de semigrupo.

(a) A imagem $f(X)$ é um subsemigrupo de Y.

(b) Se $f : (X, *, e_X) \to (Y, *, e_Y)$ é um homomorfismo de monóide, então $f(X)$ é um submonóide de Y.

(c) Se $f : (X, *, e_X) \to (Y, *, e_Y)$ é um homomorfismo de grupo, então $f(X)$ é um subgrupo de Y.

Agora considere um homomorfismo de grupo $f : X \to Y$ de um grupo $(X, *, e_X)$ para um grupo $(Y, *, e_Y)$. Como uma função $f : X \to Y$ do domínio X para o contradomínio Y, o homomorfismo $f : X \to Y$ especifica uma relação de núcleo $\ker f$ em X, com

$$x \ker f\ x' \Leftrightarrow f(x) = f(x').$$

A classe de equivalência $[e_X]_{\ker f}$ do elemento identidade e_X de X é a imagem inversa

$$f^{-1}\{f(e_X)\}.$$

Como $f : X \to Y$ é um homomorfismo de grupo, essa classe de equivalência pode ser expressa na forma

$$[e_X]_{\ker f} = f^{-1}\{e_Y\}$$

como a imagem inversa do elemento identidade e_Y do grupo de contradomínio Y.

Proposição 23 (Classe de kernel da identidade)**.** Deixe $f : (X, *, e_X) \to (Y, *, e_Y)$ ser um homomorfismo de grupo.

(a) A classe de equivalência $[e_X]_{\ker f} = f^{-1}\{e_Y\}$ forma um subgrupo N de X.

(b) Para todo x em X e n em N,

$$xnx^{-1} \in N.$$

Demonstração. Em (a) note que N não está vazio, pois contém o elemento e_X. Ainda, para os elementos n e n' de N, as propriedades homomorficas de f da

$$f(n'n^{-1}) = f(n')f(n^{-1}) = f(n')f(n)^{-1} = e_Y e_Y^{-1} = e_Y,$$

portanta N é um subgrupo de X pela proposição de teste de subgrupo.
Em (b) as propriedades homomorficas de f da

$$f(xnx^{-1}) = f(x)f(n)f(x^{-1}) = f(x)e_Y f(x)^{-1} = f(x)f(x)^{-1} = e_Y,$$

portanto xnx^{-1} está em N. ∎

Definição 28 (Subgrupos normais, grupo kernels)**.** Deixe X ser um grupo.

(a) Um subgrupo N de X satisfazendo a propriedade adicional de fechado (Item (b) da proposição anterior) é chamado de um *subgrupo normal* de X.

(b) Para um homomorfismo de grupo $f : X \to Y$ com domínio X, o subgrupo normal $f^{-1}\{e_Y\}$ de X é chamado de grupo Ker f de f.

Proposição 24 (Subgrupos normais de grupos abelianos)**.** Em um grupo abeliano G, todo subgrupo é normal.

Observação

Considere um homomorfismo de grupo $f : (G, \cdot, e_X) \to (Y, \cdot, e_Y)$. De acordo com a definição anterior (b), a classe de equivalência $[e_X]_{\ker f}$ do elemento identidade e_X de X sob a relação kernel ker f é o grupo kernel Ker f. Sendo mais geral, cada classe de equivalência sob a relação kernel ker f é uma coclasse do grupo kernel Ker f.

Proposição 25 (Classes kernel são coclasses)**.** Deixe $f : X \to Y$ ser um homomorfismo de grupo, com a relação kernel ker f e grupo kernel $N = \text{Ker } f$. Deixe x ser um elemento de X. Então a classe de equivalência $[x]_{\ker f}$ sob a relação kernel ker f é a coclasse Nx.

O mapeamento 1-1

A consideração será sobre o conjunto $A(S)$ de todos os mapeamento 1-1 de S dentro do próprio S. Vale ressaltar que mencionar um mapeamento 1-1 estamos falando sobre mapas injetivos.

Lema 8. $A(S)$ satisfaz as seguintes ocorrências

i. $[f, g \in A(S)] \implies [f \circ g \in A(S)]$

ii. $[f, g, h \in A(S)] \implies [(f \circ g) \circ h = f \circ (g \circ h)]$

iii. $f \circ i = i \circ f = f, (\forall f \in A(S))$

iv. $f \in A(S)$, $g \in A(S)$, $g = f^{-1}$ tal que $f \circ g = g \circ f = i$.

Quanto aos elementos de $A(S)$ surge uma necessidade de olharmos para eles com mais atenção. Quando S é um conjunto finito, que tem n elementos, $A(S)$ possui $n!$ elementos. Simplificando este entendimento temos que S é um conjunto que possui $s_1, s_2, \ldots, s_n$ elementos. Lembrando que $A(S)$ é um conjunto do qual possui mapeamentos 1-1 dentro de si, temos a possibilidade de enviar s_1, sob uma f, para qualquer outro elemento dentro de S. Em seguida temos um problema, que é a diminuição da possibilidade para o próximo elemento que é o s_2 ser mapeado para os outros elementos de S. Isso porque, como já vimos, f é injetiva e $f(s_1) \neq f(s_2)$. Isso significa que s_2 pode ser mapeado para qualquer outro elemento exceto em $f(x_1)$. Assim, temos que f pode enviar s_2 em $n-1$ imagens diferentes. Dessa forma, f pode enviar s_i em $n-(i-1)$ imagens diferentes. O número de f's é $n(n-1)(n-2) * s1 = n!$. O contexto disso é que queremos enviar um elemento s em n maneiras dentro do próprio S.

Exemplo 21. Pegando um número menor, $n = 3$, podemos representar manualmente o caso para $A(S) = S_3$, onde S possui s_1, s_2, s_3. Segue a ilustração dos mapeamentos dos elementos de S_3.

1. $i : s_1 \to s_1; s_2 \to s_2; s_3 \to s_3$.
2. $f : s_1 \to s_2; s_2 \to s_3; s_3 \to s_1$.
3. $g : s_1 \to s_2; s_2 \to s_1; s_3 \to s_3$.
4. $g \circ f : s_1 \to s_1; s_2 \to s_3; s_3 \to s_2$.
5. $f \circ g : s_1 \to s_3; s_2 \to s_2; s_3 \to s_1$.
6. $f \circ f : s_1 \to s_3; s_2 \to s_1; s_3 \to s_2$.

Inteiros

Definição 29 (Princípio da boa-ordenação)**.** Qualquer conjunto não vazio de inteiros não negativos possui pelo menos um elemento menor.

$$S \neq \varnothing, S \in \mathbb{Z}_+, s_0 \subset S : s_0 \leqslant S, \forall s \in S.$$

Exemplo 22. Suponha $S = \{n \in \mathbb{N} \mid 10^n < \frac{1}{2}n^n\}$, o conjunto dos números naturais n para o qual 10^n é menor que a metade de n^n. O conjunto S não está vazio, de fato infinito, à medida que n aumenta além de 10, a potência n cresce mais rápido que 10^n.

$$\lim_{x \to \infty} \left(\frac{\frac{1}{2}n^n}{10^n} \right) = \infty$$

Teorema 9 (Algoritmo de Euclides)**.**

$$m = qn + r$$

$m, n, q, r \in \mathbb{Z}$ com $n > 0$ e com $0 \leqslant r < n$.

Assumindo que se saiba trabalhar com o algoritmo de euclides, iremos prosseguir apenas com o entendimento de divisibilidade que esse teorema nos traz.

Definição 30. $m, n \in \mathbb{Z}, m \neq 0$, dizemos que m divide n, ou m é divisor de n

$$m \mid n \quad \text{válido quando} \quad n = km$$

Definição 31. Dado a, b não negativos, então o *maior divisor comum* k é definido por:

(a) $c > 0$

(b) $c \mid a \quad e \quad c \mid b$

(c) $((d \mid a) \,\&\, (d \mid b)) \rightarrow (d \mid c)$

$$k = (a, b)$$

Parafraseando, o máximo divisor comum(MDC) de um número a e b é o número positivo k do qual divide a e b, que também é divisível por qualquer número d do qual divide a e b.

Teorema 10. Sejam a, b inteiros, então o MDC $k = (a, b)$ existe, é único e é válido a equação $k = m_0 a + n_0 b$, para m_0 e n_0 adequados.

Definição 32. Dizemos que a e b são *primos relativos* se $(a, b) = 1$.

Parafraseando, é chamado de primos relativos números inteiros a e b que não possuem fator comum trivial.

Corolário 10.1. Os inteiros a e b são primos relativos *iff* $1 = ma + nb$, para m e n adequados.

Teorema 11. Se a e b são primos relativos e $a \mid bc$, então $a \mid c$.

Demonstração. Pelo colorário 10.1, $ma + nb = 1$ para algum m e n, então $(ma + nb)k = k$, isto é, $mak + nbk = k$. Assumindo que $a \mid bk$ e $a \mid mak$, então $a \mid (mak + nbk)$ e então $a \mid k$. ■

Definição 33. Um *número primo* é um inteiro $p > 1$, tal que para qualquer inteiro a, ou $p \mid a$ ou p é primo relativo a a.

Isto é, se um número p é dito primo, ou ele é divisor de um número a ou ele é primo relativo a a.

Teorema 12. Se p é um primo e $p \mid (a_1 a_2 a_3 * s a_n)$, então $p \mid a_i$ para algum i com $1 \leqslant i \leqslant n$.

Demonstração. Se $p \mid a_1$, não há o que demonstrar. No entanto, $p \nmid a_1$ nos induz a dizer que p e a_1 são primos relativos. Mas $p \mid a_1(a_2 a_3 * s a_n)$, então pelo teorema 11, $p \mid (a_2 a_3 * s a_n)$. Repetindo o argumento para a_2 chegamos a mesma redação. ■

A ideia central dos primos é entender que para todo inteiro $n > 1$ ou é um primo ou é um produto de primos. Isto é mostrado no próximo teorema.

Teorema 13. Se $n > 1$, então ou n é um primo ou n é um produto de primos.

Demonstração. Por contradição temos um inteiro $m > 1$ para o qual o teorema falha. No entanto, o conjunto M para o qual o teorema falha ele não é vazio, então, pelo princípio da boa-ordenação (Definição 29), M tem pelo menos o elemento m. Claramente, sendo $m \in M$, m não pode ser um primo, assim $m = ab$, onde $1 < a < m$ e $1 < b < m$. Isso porque $a < m$ e $b < m$ e m é o último elemento em M, nós não podemos ter $a \in M$ ou $b \in M$. Sendo $a \notin M$, $b \notin M$, pela definição de M o teorema deve ser verdadeiro para ambos a e b. Assim a e b são primos ou produto de primos; de $m = ab$ nós temos que m é um produto de primos. Isso coloca m fora de M, contradizendo que $m \in M$. Isso prova o teorema. ■

Teorema 14. Dado $n > 1$, então existe uma e somente uma maneira de escrever n na forma $n = p_1^{a_1} p_2^{a_2} * s p_k^{a_k}$, onde $p_1 < p_2 < \ldots < p_k$ são primos e as potências $a_1, a_2, \ldots a_k$ são todos positivos.

Demonstração. Novamente, por contradição assumimos que o teorema falha e que se tenha ao menos um inteiro $m > 1$ para o qual o teorema é falso. Esse m deve possuir duas fatorizações distintas como $m = p_1^{a_1} p_2^{a_2} * s p_k^{a_k} = q_1^{b_1} q_2^{b_2} * s q_l^{b_l}$ onde $p_1 < p_2 < \ldots < p_k$, $q_1 < q_2 < \ldots < q_l$ são primos e onde as potências $a_1, \ldots, a_k$ e $b_1, \ldots, b_l$ são todos positivos. Sendo $p_1 \mid p_1^{a_1} * s p_k^{a_k} = q_1^{b_1} * s q_l^{b_l}$, pelo teorema 12 $p_1 \mid q_i^{b_1}$ para algum i; assim, também pelo teorema 12 $p_1 \mid q_i$, temos $p_1 = q_i$. Pela mesma razão $q_1 = p_j$ para algum j; assim $p_1 \leqslant p_j = q_1 \leqslant q_i = p_1$. Isso nos da que $p_1 = q_1$. Agora sendo $\frac{m}{p_1} < m$, $\frac{m}{p1}$ tem a propriedade de fatoração unica. Mas $\frac{m}{p_1} = p_1^{a_1 - 1} p_2^{a_2} * s p_k^{a_k} = q_1^{b_1 - 1} q_2^{b_2} * s q_l^{b_l}$ uma vez que $\frac{m}{p_1}$ pode ser fatorado em uma e apenas uma maneira em $a_2 = b_2, \ldots, a_k = b_k$. Os primos e seus potências que surgem na fatorização de m são únicos. Isso contradiz a unicidade para m, o que prova o teorema. ■

Estes dois teoremas nos diz que podemos construir inteiros de primos em uma maneira muito precisa e bem definida. Também nos leva ao ponto da criação de MUITOS primos...

Teorema 15. Existe um número infinito de primos.

Demonstração. Por contradição nós podemos enumerar todos os primos em $p_1, p_2, \ldots p_k$. Considere o inteiro $q = 1 + p_1 p_2 * s p_k$. Uma vez que $q > p_i$, pois obtemos um resto de 1 ao dividir q por p_i, q não é divisível por nenhum $p_1, \ldots, p_k$. Então q não é um primo e também não é divisível por nenhum primo. Ora, isso viola o teorema 13 , portanto prova o teorema. ■

Para exercício, segue os itens

1. Mostre que nenhum inteiro $u = 4n + 3$ pode ser escrito como $u = a^2 + b^b$, onde a, b são inteiros.
2. Se T é um subconjunto infinite de $\mathbb{N}$, o conjunto de todos os inteiros positivos, mostre que existe um mapeamento $1 - 1$ de T em $\mathbb{N}$.
3. Se p é um primo, prove que não se pode encontrar inteiros não nulos a e b tal que $a^2 = pb^2$.(Isso mostra que a raiz quadrada de um número primo é irracional.)

Indução Matemática

Um método muito útil para verificarmos resultados quando trabalhamos com problemas sobre os inteiros.

Teorema 16. Deixe $P(n)$ ser uma declaração sobre os inteiros positivos tal que:

i. $P(1)$ é verdadeiro.

ii. Se $P(k)$ for verdadeiro para algum inteiro $k \geqslant 1$, então $P(k + 1)$ também é verdadeiro. (*passo indutivo*)

Portanto $P(n)$ é verdadeiro para todo $n \geqslant 1$.