Notas em matemática

Algebra

Douglas Santos
douglass@ufrj.br

04/2022

Conteúdo

Mapeamento

Função Geral

Definição 1
Se $g : X \to Y$ e $f : Y \to Z$, então a *composição*, denotada por $f \circ g$, é o mapameanto $f \circ g : X \to Z$ definido por $(f \circ g)(x) = f(g(x))$ para todo $x \in X$.

Lema 1
Se $h : X \to Y$, $g : Y \to Z$ e $f : Z \to W$, 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.
$\forall x \in X, (f \circ (g \circ h))(x) = ((f \circ g) \circ h)(x)$. A aplicação da definição de composição segue

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

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

$$(f \circ (g \circ h))(x) = ((f \circ g) \circ h)(x), \forall x \in X.$$

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

$$f \quad e \quad g \quad em \quad S \quad implica \quad g \circ f \quad em \quad S.$$

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

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

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

$$id_Y \circ f = f = f \circ id_X.$$

Definição 4 (Monoide de Funções)
Um conjunto S de auto-mapas em um conjunto base X é dito ser um Monoide 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 Monoide 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 $id_{\mathbb{R}^1_2}$, então $L(2, \mathbb{R})$ forma um Monoide 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 contra-domínio 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

$$r \circ f = id_X.$$

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

$$r \circ f(x) = r\,(f(x)) = x_{f(x)} = x = id_X(x),$$

que verifica $r \circ f = id_X$. ∎

Definição 6 (Retração)
Um mapeamento $r : Y \to X$ é cahamado de uma retração de uma função $f : X \to Y$ se $r \circ f = id_X$.

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 $abs : \mathbb{Z} \to \mathbb{N}; n \mapsto\mid n \mid$

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 elementos 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. Uma função bijetiva $f : X \to X$ é chamada de uma permutação do conjunto X.

ii. 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 Monoide 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 núcleo 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 núcleo (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 núcleo 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 $\backslash : X \to \mathbb{R}; (n, m) \mapsto n^{-1}m$ (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

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

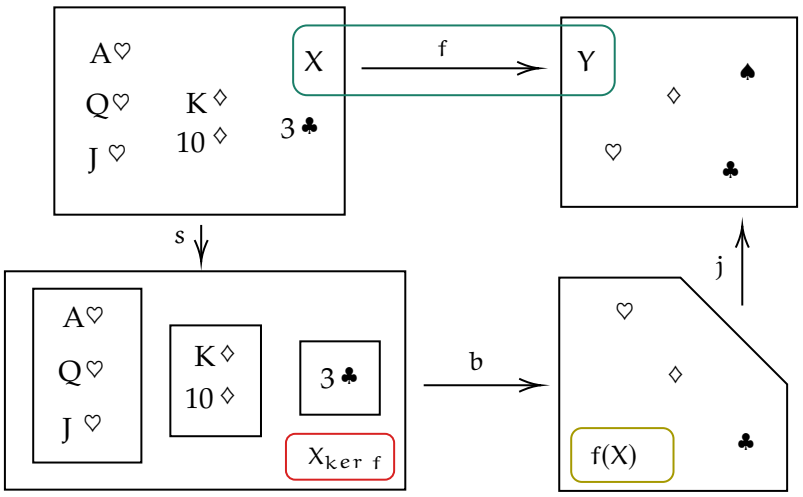


Ilustração do Primeiro Teorema de Isomorfismo.

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.

Aritmética Modular

Considere $a = dq + r$ $(0 \leqslant r < d)$. Sendo a o dividendo, q o quociente, d o divisor e o r o resto. Para cada inteiro a, define-se $(a \bmod b)$ por

$$a = qd + (a \bmod d). \tag{1}$$

Logicamente $(a \bmod d)$ representa o resto. Agora considere a função

$$f : \mathbb{Z} \to \mathbb{N}; \quad a \mapsto a \bmod d. \tag{2}$$

As classes de núcleo $[a]_{\bmod d}$ dessa função são conhecidas como *classes de congruência módulo d*. Dois inteiros a e d são ditos serem *congruentes módulo* d, denotado por

$$a \equiv b \pmod d, \tag{3}$$

se eles estão relacionado pela relação de núcleo $\ker f$, ou (equivalentemente) se eles estão na mesma classe de congruência, ou se eles deixam o mesmo resto após a divisão por d. Para facilitar o uso de 3 será util resumir mais formas equivalentes da relação.

Proposição 9 (Caracterização de Congruência)
Seja d um inteiro positivo. Para inteiros a e b, são equivalentes:

(a) $a \equiv b \pmod b$;

(b) $d \mid a - b$;

(c) $a - b$ é um múltiplo de d.

A bijeção b do primeiro teorema de isomorfismo para conjuntos provê um isomorfismo

$$\begin{aligned} \mathbb{Z}_{\bmod d} &\to \frac{\mathbb{Z}}{d} \\ [a]_{\bmod d} &\mapsto a \bmod d. \end{aligned}$$

entre o conjunto das classes de congruência módulo d e o conjunto

$$\frac{\mathbb{Z}}{d} = \{0, 1, 2, \ldots, d-1\}$$

dos restos ou inteiros módulo d, a imagem da função 2. O isomorfismo é frequentemente usado para identificar uma classe de congruência com seu resto representativo, assim o conjunto das classes de congruência é então escrito como $\frac{\mathbb{Z}}{d}$.

Para $d = 2$ o conjunto $\frac{\mathbb{Z}}{2} = \{0, 1\}$ consiste de *dois bits* ou *digitos binários* 0 e 1.

Proposição 10
Seja d um inteiro positivo. Suponha que para inteiros a_i e b_i $(i = 1, 2)$,

$$a_1 \equiv b_1 \mod d \quad \& \quad a_2 \equiv b_2 \mod d.$$

Então

$$a_1 + a_2 \equiv b_1 + b_2 \mod d \quad \& \quad a_1 \cdot a_2 \equiv b_1 \cdot b_2 \mod d.$$

Corolário 3.1
Existem operações *bem definidas*

$$[a]_{\mod d} + [b]_{\mod d} = [a + b]_{\mod d} \tag{4}$$

e

$$[a]_{\mod d} \cdot [b]_{\mod d} = [a \cdot b]_{\mod d} \tag{5}$$

nos conjuntos $\mathbb{Z}_{\mod d}$ e $\frac{\mathbb{Z}}{d}$.

Note que para cada elemento a de $\frac{\mathbb{Z}}{d}$, a função

$$\frac{\mathbb{Z}}{d} \to \frac{\mathbb{Z}}{d};\ x \mapsto a + x$$

é a permutação

$$((0 \mod d)\ (1 \mod d)\ (2 \mod d)\ \ldots\ (-1 \mod d))^a$$

do grupo cíclico C_d.

Grupos e monoides

Tomando um conjunto S não vazio e "equipando-o"com uma operação podemos combinar, de várias formas (geralmente em duas), os elementos desse conjunto S. Combinar os elementos de S pode ser denominado como *operações em* S. Uma coisa importante é saber 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.

As estruturas abstratas

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

$$\begin{aligned} S \times S &\to S \\ (g, f) &\mapsto g \circ f. \end{aligned}$$

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.

Definição 14 (Magma)
Seja M um conjunto com uma operação $*$ que mapeia dois elementos $x, y \in M$ para $x * y$. Para termos um magma basta o conjunto M e a operação $*$ satisfazerem a propriedade de ser fechado. Com efeito,

$$\begin{aligned} * : M \times M &\to M \\ (x, y) &\mapsto x * y \end{aligned}$$

onde $x * y \in M$. O conjunto M é fechado com respeito a operação $*$.

Definição 15 (Semigrupos)
Seja S um conjunto equipado com a operação $*$.

$$\begin{aligned} * : S \times S &\to S \\ (x, y) &\mapsto g * f \end{aligned}$$

S é fechado com respeito a operação binaria $*$ em S. Isto é, S possui um magma. 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 os elementos x, y e z do conjunto S.

Definição 16 (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
Seja S um 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. Com efeito, $S := \{x \in \mathbb{R} \mid x > 1\}$ forma um semigrupo multiplicativo.

Exemplo 6
Seja $A := \{x \in \mathbb{Z} \mid x < 0\}$

$$\begin{aligned} A \times A &\to A \\ (x_1, x_2) &\mapsto x_1 - x_2. \end{aligned}$$

A não forma um semigrupo, pois a operação em A não é associativa. Isto é, a subtração nao é associativa. De fato,

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

enquanto

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

monoides

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

Definição 17 (monoides abstratos)
Seja $(M, *)$ um semigrupo. Então M é dito ser um *monoide* (ou um *monoide abstrato*) $(M, *, e)$ se ele conter um elemento e satisfazendo

$$e * x = x = x * e \quad \forall x \in M.$$

O elemento e é conhecido como o *elemento neutro* do monoide M.

Em essência, um monoide contém um semigrupo com um elemento neutro.

Exemplo 7
O conjunto $S := \{x \in \mathbb{R} \mid x > 1\}$ com a operação multiplicativa do exemplo anterior não forma um monoide. Certamente S não contém o elemento neutro 1 para a multiplicação dos números reais. De fato, para todo elemento de S teremos $x * y > x$.

Proposição 11 (Unicidade do elemento neutro)
Seja M um monoide. Se e e f são elementos neutros de M, então $e = f$. Isto é, o elemento neutro é único.

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

Grupos

Definição 18 (Grupos Abstratos)
Um monoide $(G, *, e)$ 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 operação $*$ 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,
Magmas precisam satisfazer a propriedade fechado.
Semigrupos precisam satisfazer as propriedades fechado e associatividade.
monoides precisam satisfazer as propriedades fechado, associatividade e identidade.
Grupos precisam satisfazer as propriedades fechado, associatividade, identidade e inverso. Ou, equivalentemente, um grupo G possui um magma inverso, associatividade e um elemento neutro.

Proposição 12 (Unicidade dos inversos)
Em um grupo G, cada elemento x tem um único inverso.

Demonstração. Se tiver mais de um inverse x, i.e, $\exists y \in G$ tal que $x * y = y * x = e$. Temos $x * x^{-1} = x^{-1} * x = e$. Desenvolvendo com ambas teremos: $y = y * e = y * (x * x^{-1}) = (y * x) * x^{-1} = e * x^{-1} = x^{-1}$. ■

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

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

Exemplo 10
Considera a função bijetiva $f : X \to X$. Caso X tenha um número finito n de elementos, f será denotada por S_n e será chamada de *grupo simétrico* ou *grupo das permutações* de n letras. Temos que $\#S_n = n!$. O grupo S_3:

$$S_3 = \left\{ \begin{pmatrix} 123 \\ 123 \end{pmatrix}, \begin{pmatrix} 123 \\ 213 \end{pmatrix}, \begin{pmatrix} 123 \\ 321 \end{pmatrix}, \begin{pmatrix} 123 \\ 132 \end{pmatrix}, \begin{pmatrix} 123 \\ 231 \end{pmatrix}, \begin{pmatrix} 123 \\ 312 \end{pmatrix} \right\},$$

onde a notação $\left(\begin{smallmatrix} 123 \\ abc \end{smallmatrix}\right)$ representa a função definida da maneira seguinte: $f(1) = a$, $f(2) = b$ e $f(3) = c$.

Definição 19 (Elementos invertíveis)
Seja $(M, *, e)$ um monoide. Um elemento x de M é dito um invertível ou uma unidade se existe um elemento y de M tal que $x \cdot y = e = y \cdot x$.

Proposição 13 (Elementos invertíveis formam um grupo)
Seja $(M, *, e)$ um monoide. Então o conjunto M^* dos elementos invertíveis de M forma um grupo $(M^*, *, e)$.

Definição 20 (O grupo de unidades)
Para um monoide $(M, *, 1)$, o grupo $(M^*, *, 1)$ é conhecido como o grupo de unidades do monoide M.

Exemplo 11
Os inteiros formam um monoide comutativo $(\mathbb{Z}, \cdot, 1)$ sob a multiplicação. O conjunto dos invertíveis do monoide de inteiros é $\{\pm 1\}$.

Exemplo 12
A notação da definição anterior (M^*) é consistente com o Exemplo 9: o conjunto dos invertíveis do monoide dos números reais sob a multiplicação é o conjunto $\mathbb{R}^*$.

Potências

Considere os conjunto de funções $f : X \to S$ de um certo domínio X para um contradomínio S carregando uma estrutura algebrica. A soma $f + g$ de duas funções reais $f : \mathbb{R} \to \mathbb{R}$ e $g : \mathbb{R} \to \mathbb{R}$ é determinada por

$$(f + g)(x) = f(x) + g(x), \quad \forall x \in \mathbb{R}.$$

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 neutro), e a inversa da função f dada pela negação $-f$, teremos

$$(-f)(x) = -f(x), \quad x \in \mathbb{R}.$$

Definição 21 (Estrutura das potências)
Sejam X e S conjuntos. Considere o conjunto S^X de todas as funções $f : X \to S$.

(a) Se S carrega uma estrutura de Semigrupo $(S, *)$, então a 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

$$(f \cdot g)(x) = f(x) \cdot g(x), \quad \forall x \in X.$$

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

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

Exemplo 13 (Vetores)
Seja n um inteiro positivo. Um vetor real com n componentes (ou vetor de dimensão n) 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.

Submonoides e Subgrupos

Definição 22 (Subsemigrupos)
Sejam $(S, *)$ um semigrupo e X um subconjunto de S. Então X é descrito como um subsemigrupo do semigrupo $(S, *)$ se ele for fechado sob $*$:

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

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 14 (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. Por outro lado, o conjunto dos inteiros ímpares não forma um subsemigrupo, pois a propriedade fechado é violada, por exemplo, por $1 + 3$.

Definição 23 (Submonoides)
Um subconjunto X de um monoide $(M, *, e)$ é um submonoide se ele é um subsemigrupo do semigrupo $(M, *)$ e se ele conter o elemento neutro e de M.

Se $(X, *, e)$ é um submonoide de um monoide $(M, *, e)$, então $(X, *, e)$ é um monoide: 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 neutro é um submonoide de qualquer monoide $(M, *, e)$ com e como elemento neutro.

Exemplo 15 (Submonoides de inteiros sob a operação de adição)
O subsemigrupo de inteiros negativos não forma um submonoide do monoide $(\mathbb{Z}, +, 0)$ de inteiros sob a adição, pois ele não contém o elemento neutro 0 de $\mathbb{Z}$. Por outro lado, o monoide $(\mathbb{N}, +, 0)$ dos números natural sob a adição forma um submonoide de $(\mathbb{Z}, +, 0)$.

Exemplo 16 (Matrizes Estocásticas)
Uma matriz real quadrada de ordem 2

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

é dita estocástica se p_1, p_2, q_1, q_2 não são negativos:

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

A matriz identidade I_2 é estocástica. Seja Π_2^2 o conjunto das matrizes estocásticas. Então Π_2^2 forma um submonoide do monoide $\mathbb{R}_2^2$ de todas as matrizes quadradas de ordem 2 sob a operação de multiplicação de matrizes.

Definição 24 (Subgrupos)
Um submonoide X de um grupo $(G, *, e)$ é um subgrupo (notação: $X \leqslant G$) de G se ele é fechado sob a inversão em G:

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

O conjunto $\{e\}$ consistindo apenas do elemento neutro é um subgrupo de qualquer grupo $(G, *, e)$ com e sendo seu elemento neutro. Como um subgrupo tem que ser um submonoide com um elemento neutro, ele também tem que ser não vazio. O teste de subgrupo é uma maneira rápida para checar se um subconjunto X não vazio de um grupo G forma um subgrupo de G.

Proposição 14 (O teste do subgrupo)
Seja X 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. 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 neutro $e = a * a^{-1}$ 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 4 (Subgrupos de inteiros)
Seja J um subgrupo do grupo $(\mathbb{Z}, +, 0)$. Então existe um número natural d tal que J consiste do conjunto $d\mathbb{Z}$ de múltiplos inteiros de d.

Teorema 5 (Interseção de Subgrupos)
Seja $(G, *)$ um grupo e H, K subgrupos de G. Então, $H \cap K \leqslant G$.

Demonstração. Hipótese: Para $a, b \in H \cap K$ tem-se $a * b^{-1} \in H \cap K$
Sejam $a, b \in H \cap K$. Então $a \in H$ e $a \in K$. Da mesma forma, $b \in H$ e $b \in K$. Se $a, b \in H$ então $a * b^{-1} \in H$, pois $H \leqslant G$.
Da mesma forma, se $a, b \in K$, então $a * b^{-1} \in K$. Mas se $a * b^{-1} \in H$ e $a * b^{-1} \in K$, então $a * b^{-1} \in H \cap K$. ■

Teorema 6 (Generalização da Interseção de Subgrupos)
Seja $(G, *, e)$ um grupo e $H_1, H_2, ..., H_n$ subgrupos de G, Então

$$H_1 \cap H_2 \cap \cdots \cap H_n \leqslant G.$$

Proposição 15
A união de subgrupos pode não ser subgrupo.

Proposição 16 (Grupos de ordem primo)
Um grupo com um número primo de elementos não pode ter subgrupos próprios e não triviais.

Proposição 17 (Cancelação em grupos)
Seja G 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.

Coclasse (ou Cosets)

Um semigrupo $(S, *)$ carrega uma operação associativa de seus elementos. É útil extender essa operação para subconjuntos de S.
Seja X um subconjunto de um semigrupo $(S, *)$. Se s é um elemento de S, define-se

$$Xs = \{xs \mid x \in X\} \quad \text{e} \quad sX = \{sx \mid x \in X\}.$$

Esses conjuntos, respectivamente, são a *coclasse à direita* e a *coclasse à esquerda* do subconjunto X com o elemento s. Por exemplo, o subgrupo $d\mathbb{Z}$ do grupo $(\mathbb{Z}, +, 0)$ é a coclasse de d no semigrupo $(\mathbb{Z}, \cdot)$. Se X é um subconjunto de um monoide M com o elemento neutro e, então as coclasses eX e Xe coincidem com o subconjunto X.

Exemplo 17
Considere um semigrupo $S = (\mathbb{Z}_8, +)$ e um subconjunto de $\mathbb{Z}_8$ $X = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$. Coclasse à esquerda tomando $\overline{1} \in G$: $\overline{1} + X = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$. Coclasse à direita tomando $\overline{2} \in G$: $X + \overline{2} = \{\overline{2}, \overline{4}, \overline{6}, \overline{0}\}$.

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

Corolário 6.2 (Coclasses finitas são todas do mesmo tamanho)
Seja X 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 18
Seja H um subgrupo de um grupo G.

a. Define-se uma relação R em G por

$$g_1 R g_2 \quad \text{sss} \quad hg_1 = g_2 \quad \text{para algum} \quad h \in H.$$

Então R é uma relação de equivalência em G.

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

Teorema 7 (Teorema de Lagrange)
Seja H um subgrupo de um grupo finito G. Então o número $| H |$ divide o número $| G |$.

Demonstração. Pela proposição 18 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 em 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.

Exemplo 18
$G = (\mathbb{Z}_6, +)$ e $H = (\mathbb{Z}_1, +)$

$$\frac{| G |}{| H |} = \frac{6}{2} = 3.$$

Observação

- Se H for um subconjunto próprio, denotamos o subgrupo como $H < G$ (por exemplo, $(\mathbb{Z}, +) < (\mathbb{R}, +)$).
- Se G é um grupo, então G é um **subgrupo impróprio** de G e todos os demais são **subgrupos próprios**.
- TODO grupo admite *pelo menos dois* subgrupos (G e $H = \{e\}$). Estes são os **subgrupos triviais**.
- Um subgrupo H é próprio se ele não for impróprio.

Como primos são números irredutíveis, o teorema de Lagrange produz o seguinte resultado.

Homomorfismo

Estudar conjuntos nos leva a estudar funções entre conjuntos. Similarmente acontece quando estudamos estruturas algébricas como semigrupos, monoides 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 de potenciação,

$$E(x + y) = e^{x+y} = e^x \cdot e^y = E(x) \cdot E(y). \tag{6}$$

Aqui o domínio da função exponencial E é o semigrupo $(\mathbb{R}, +)$. O contradomínio da função E é o semigrupo $(\mathbb{R}, \cdot)$.
A equação (6) 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. Obtem-se a mesma resposta nas duas formas.

Definição 25 (Homomorfismo de semigrupos, monoides e grupos)
Homomorfismo e isomorfismo.

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

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

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

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

$$X \cong Y.$$

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

Exemplo 19
Seja $\phi : (X, *, e) \to (Y, \star, f)$ um isomorfismo dos grupos X e Y. Mostre que ϕ transforma subgrupo em subgrupo.

Demonstração. Sendo $\phi : X \to Y$ um isomorfismo, isto é, um homomorfismo sobrejetor, então $\phi(x*y) = \phi(x) \star \phi(y)$ e ϕ é uma bijeção.
Se $H \leqslant X$ então $\phi(H) = \{y \in X'; y = \phi(x), x \in H\}$.
$\vdash \phi(H) \leqslant X'$.
Sejam $u, v \in \phi(H)$. Então $u = \phi(a)$ $v = \phi(b)$ onde $a, b \in H$.
Assim, $u \star v^{-1} = \phi(a) \star [\phi(b)]^{-1}$
Dai $u \star v^{-1} = \phi(a) \star \phi(b^{-1}) = \phi(a * b^{-1})$
Ou seja, $u \star v^{-1}$ é imagem de um elemento de H e, portanto, $u \star v^{-1} \in \phi(H)$. ■

Exemplo 20
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 monoide de um monoide dos números reais sob a operação de adição para o monoide dos números reais sob a operação de multiplicação.

Exemplo 21 (Inclusão de um subgrupo)
Seja H 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 22
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, monoides ou grupos então as projeções são homomorfismos de semigrupos, monoides, e grupo recpetivamente.

Proposição 19 (Homomorfismo de semigrupo entre grupos)
Seja $\phi : (X, \circ) \to (Y, *)$ 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 neutro 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 monoide.
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 8 (Homomorfismo de monoide e grupo de unidades)
Seja $\phi : (M, \circ, e) \to (N, *, f)$ um homomorfismo de monoide. 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 $bemM$. 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 20 (O gráfico de um homomorfismo)
Seja $(X.\circ)$ 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 8.1
Seja $(X, \circ, e)$ e $(Y, *, f)$ serem monoides. Então uma função $f : X \to Y$ é dita um homomorfismo de monoide se e somente se o gráfico um submonoide do produto direto de monoide $X \times Y$.

Subgrupo Normal

Seja $f : X \to Y$ 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, monoides ou de grupos, a imagem irá carregar a correspondente estrutura algebrica.

Proposição 21 (Imagens de homomorfismos)
Seja $f : (X, *) \to (Y, *)$ 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 monoide, então $f(X)$ é um submonoide 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 neutro 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 neutro e_Y do grupo de contradomínio Y.

Proposição 22 (Classe de núcleo da identidade)
Seja $f : (X, *, e_X) \to (Y, *, e_Y)$ 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

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

portanto 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 26 (Subgrupos normais / grupo de núcleos (Group Kernel))
.

- Um subgrupo N de um grupo X diz-se um *subgrupo normal* de X se $xN = Nx, \forall x \in X$. A notação $N \trianglelefteq X$ pode ser usada.
- O núcleo de um homomorfismo de grupo $\phi : (G, *, e) \to (G', \circ, f)$ é o conjunto de todos os elementos de G dos quais são mapeados para o elemento neutro de G'. O núcleo é um subgrupo normal de G e sempre contém o elemento neutro de G. É reduzido para o elemento neutro se e somente se ϕ é injetiva.

Seja X 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 (Grupo núcleo) de f.

Isto é, N é normal em X **iff** $xNx^{-1} \subseteq N$.

Demonstração. Se N é normal em X, então para quaisquer $x \in X$ e $n \in N$, existe $n' \in N$ tal que $xn = n'x$. Logo $xnx^{-1} = n'$ e, portanto, $xNx^{-1} \subseteq N$. Reciprocamente, se $xNx^{-1} \subseteq N, \forall x \in X$, então, tomando $x = a$, tem-se $aN \subseteq Na$. Por outro lado, tomando $x = a^{-1}$, tem-se $a^{-1}N(a^{-1})^{-1} = a^{-1}Na \subseteq N$, isto é, $Na \subseteq aN$. ■

Proposição 23 (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 neutro e_X de X sob a relação núcleo $\ker f$ é o grupo núcleo Ker f. Sendo mais geral, cada classe de equivalência sob a relação núcleo $\ker f$ é uma coclasse do grupo núcleo Ker f.

Proposição 24 (Classes de núcleo são coclasses)
Seja $f : X \to Y$ um homomorfismo de grupo, com a relação núcleo $\ker f$ e grupo núcleo $N = \text{Ker } f$. Seja x um elemento de X. Então a classe de equivalência $[x]_{\ker f}$ sob a relação núcleo $\ker f$ é a coclasse Nx.

Demonstração. Para provar a igualdade dos dois conjuntos $[x]_{\ker f}$ e Nx seguiremos mostrando que cada um está contido no outro.
Primeiramente, considere um elemento y da classe de equivalência $[x]_{\ker f}$, onde $f(x) = f(y)$.
Então, pela propriedade homomorfica de f,

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

onde yx^{-1} é algum membro n de $N = f^{-1}\{e_Y\}$.
Como $xy^{-1} = n$, nós obtemos y como o membro nx da coclasse Nx.
Por outro lado, considere um membro nx da coclasse Nx, com $n \in N$. Então

$$f(nx) = f(n)f(x) = e_Y f(x) = f(x),$$

onde nx $(\ker f)x$, e $nx \in [x]_{\ker f}$ pela simetria (propriedade simétrica) de $\ker f$. ■

Quocientes

Para subconjuntos A e B de um grupo $(X, \cdot, e_x)$ considere a multiplicação

$$A \cdot B = \{ab \mid a \in A, b \in B\}$$

Proposição 25 (Reconhecendo subgrupos)
Seja X um grupo.

(a) A multiplicação é associativa.

(b) Um subconjunto não vazio H de X é um subgrupo *IFF* $H \cdot H = H$ e $H^{-1} = H$.

O item *(a)* é imediato, basta considerar a multiplicação feita com os conjuntos A e B juntamento com outro conjunto C, sendo os três subconjuntos de X. Supondo que H é um subgrupo, segue que $H \cdot H \subseteq H$ por ser fechado sob a multiplicação. Reciprocamente, cada elemento h de H pode ser escrito como $e \cdot h$ em $H \cdot H$. Também $H^{-1} \subseteq H$ pois H é fechado sob a inversão. Por outro lado, cada elemento h de H pode ser escrito como o elemento $(h^{-1})^{-1}$ de H^{-1}.

Proposição 26 (Coclasses de subgrupos normais)
Seja N um subgrupo normal de um grupo X. Então o conjunto

$$X/N = \{Nx \mid x \in X\}$$

de coclasses a direita é um grupo $(X/N, \cdot, N)$ sob a multiplicação (associativa), com

$$(Nx)^{-1} = Nx^{-1}$$

para $x \in X$.

Corolário 8.2
Seja N um subgrupo normal de um grupo X. Então existe um homomorfismo

$$\begin{aligned} X &\to X/N \\ x &\mapsto Nx. \end{aligned}$$

com o grupo núcleo N.

Definição 27 (Grupos quocientes)
Sejam X um grupo e $N \trianglelefteq X$. Então o grupo

$$(X/N, \cdot, N)$$

da proposição 26 é chamado de quociente de X pelo subgrupo normal N.

Exemplo 23 (Arimética Modular)
Seja d um inteiro positivo. No grupo $(\mathbb{Z}, +, 0)$ dos inteiros sob a operação de adição, o subgrupo $d\mathbb{Z}$ dos multiplos de d é normal. O grupo quociente $\mathbb{Z}/d\mathbb{Z}$ é o conjunto $\mathbb{Z}_{\mathrm{mod}\ d}$, com a adição

$$(d\mathbb{Z} + a) + (d\mathbb{Z} + b) = d\mathbb{Z} + (a + b).$$

As inversas são dada pela negação

$$-(d\mathbb{Z} + a) = d\mathbb{Z} - a,$$

enquanto o elemento neutro é o subgrupo $d\mathbb{Z}$. De fato, o conjunto $Z/d\mathbb{Z}$ carrega mais estrutura, a multiplicação

O primeiro teorema de isomorfismo para Grupos

Teorema 9
Seja $f : (X, \cdot, e_X) \to (Y, \cdot, e_Y)$ um homomorfismo de grupo.

(a) O grupo núcleo $N = f^{-1}\{e_Y\}$ é um subgrupo normal do grupo do domínio X.

(b) A imagem f(X) é um subgrupo do grupo contradomínio Y.

(c) Na fatorização

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

dada pelo primeiro teorema de isomorfismo para conjuntos, a sobrejeção s pode ser tomada como o homomorfismo sobrejetivo

$$s : X \to X/N;\ x \mapsto Nx$$

do corolário 8.2, a bijeção b é o isomorfismo de grupo bem definido

$$b : X/N \to f(X);\ Nx \mapsto f(x)$$

do quociente X/N para a imagem f(X), e a injeção j é o isomorfismo de grupo injetivo

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

Se o domínio (do homomorfismo de grupo) no primeiro teorema de isomorfismo é finito, então a bijeção b pode ser usada para contar o tamanho da imagem.

Corolário 9.1
Seja $f : X \to Y$ um homomorfismo de grupo com o grupo núcleo N e de domínio finito X. En toa o tamanho $|\ f(X)\ |$ da iamgem de f é o índice

$$|\ X/N\ | = |\ X\ | \ /\ |\ N\ |$$

do subgrupo N de X.

Exemplo 24 (O grupo linear especial)
Considere o homomorfismo de grupo

$$\begin{aligned} \det : GL(2,\mathbb{R}) &\to \mathbb{R}^* \\ \begin{bmatrix} a & b \\ c & d \end{bmatrix} &\mapsto\ ad - bc. \end{aligned}$$

O grupo núcleo é o conjunto $SL(2,\mathbb{R})$ das matrizes reais 2×2 de determinante 1. Esse grupo $SL(2,\mathbb{R})$ é chamado de *grupo linear especial* (real) de dimensão 2. O primeiro teorema de isomorfismo para grupos exibe o isomorfismo

$$\frac{GL(2,\mathbb{R})}{SL(2,\mathbb{R})} \cong \mathbb{R}^*$$

do grupo quociente para o grupo dos números reais sem o zero sob a multiplicação.

Teorema 10 (Teorema do resto chinês)
Seja a e b serem coprimos ($MDC(a, b) = 1$) inteiros positivos. Então existem isomorfismos

$$\frac{\mathbb{Z}}{ab\mathbb{Z}} \cong \frac{\mathbb{Z}}{a\mathbb{Z}} \times \frac{\mathbb{Z}}{b\mathbb{Z}}$$

de conjuntos, grupos sob a operação de adição, e monoides sob a operação de multiplicação.

Demonstração. É claramente bem definido, pois

$$ab \mid (x - x') \implies a \mid (x - x') \wedge b \mid (x - x').$$

É certamente um homomorfirmo de (semi)grupo e monoide. Para um elemento $ab\mathbb{Z} + x$ do grupo núcleo $\mathrm{Ker}\ p$, o inteiro representativo x é um múltiplo de ambos a e b. Como a e b são coprimos ($MDC(a, b) = 1$), o menor múltiplo comun deles é ab. Assim $ab \mid x$, e o grupo núcleo $\mathrm{Ker}\ p$ é trivial. Segue que o homomorfismo de grupo é injetivo, pois as classes da relação núcleo $\ker p$ são cocalsses do subgrupo $\mathrm{Ker}\ p$. Como o domínio e o contradomínio tem o mesmo número finito de elementos, o corolário 9.1 mostra que o mapa p é sobrejetivo. ■

Lei dos expoentes

Seja x um elemento de um monoide $(M, \cdot, e)$. Então para números naturais n, as potências x^n são definidas recursivamente por

$$x^0 = e \quad \& \quad x^{n+1} = x^n \cdot x. \tag{7}$$

No monoide $(\mathbb{N}, +, 0)$ dos números naturais sob a operação de adição, a notação de potência x^n para um número natural x se traduz para a notação de multiplicação nx.
Geralmente, para um monoide $(M, +, 0)$ (comutativo) escrito usando a notação aditiva, a definição recursiva (7) das potências se traduz para a definição recursiva

$$0x = 0 \quad \& \quad (n + 1)x = nx + x$$

dos multiplos.

Teorema 11 (Universalidade dos números naturais)
Seja x um elemento de um monoide $(M, \cdot, e)$. Então existe um *único homomorfismo de monoide*

$$f : (\mathbb{N}, +, 0) \to (M, \cdot, e);\ n \mapsto x^n \tag{8}$$

com $f(1) = x$.

Demonstração. O mapa f de (8) é um homomorfismo de monoide, pois

$$f(0) = x^0 = e$$

pela definição, e

$$f(m + n) = x^{m+n} = x^m \cdot x^n = f(m) \cdot f(n)$$

para números naturais m e n pela regras da potência. Agora suponha que $\varphi : (\mathbb{N}, +, 0) \to (M, \cdot, e)$ é um homomorfismo de monoide com $\varphi(1) = x$. Para números naturais n, a equação $\varphi(n) = f(n)$ segue pela indução em n. Certamente $\varphi(0) = e = f(0)$, pois φ é um homomorfismo de monoide. Então se $\varphi(n) = f(n)$, nós temos

$$\varphi(n + 1) = \varphi(n) \cdot \varphi(1) = \varphi(n) \cdot x = f(n) \cdot x = x^n \cdot x = x^{n+1} = f(n + 1),$$

a primeira equação é válida pois φ é um homomorfismo de semigrupo. ■

Agora Seja x um elemento de um grupo $(G, \cdot, e)$. Para cada inteiro positivo n, define $x^{-n} = (x^{-1})$.

Teorema 12
Suponha que x é um elemento de um grupo $(G, \cdot, e)$. Então existe um único homomorfismo de grupo

$$E_x : (\mathbb{Z}, +, 0) \to (G, \cdot, e);\ n \mapsto x^n \tag{9}$$

com $E_x(1) = x$.

Exemplo 25 (Exponenciação)
Considere o elemento e do grupo $(\mathbb{R}, \cdot, 1)$ dos números reais sem o zero sob a operação de multiplicação. Então

$$E_x(n) = e^n$$

para cada inteiro n. Para o elemento 2 de $\mathbb{R}^*$, nós temos $E_2(n) = 2^n$ para cada inteiro n. Assim, o homomorfismo de grupo exclusivamente especificado (9) pode ser considerado como uma "expoenciação de base x"no grupo G.

Na universalidade dos inteiros o grupo núcleo $Ker(E_x)$ do homomorfismo E_x é um subgrupo do grupo $(\mathbb{Z}, +, 0)$ dos inteiros. Pelo teorema de subgrupos de inteiros (onde temos o conjunto $d\mathbb{Z}$, multiplos de d) o grupo $Ker(E_x)$ é o conjunto dos multiplos de um número natural d_x.

Definição 28 (Grupo cíclico gerado, Ordem do elemento)
Seja x um elemento de um grupo $(G, \cdot, e)$.

(a) A imagem $\langle x \rangle$ do homomorfismo de grupo E_x em (9) é chamada de subgrupo cíclico de G gerado por x.

(b) Se $d_x = 0$, o elemento x é dito ser de *ordem infinita*.

(c) Se d_x é um inteiro positivo, o elemento x é dito ser de *ordem finita* d_x.

No primeiro teorema de isomorfismo para grupos ((b); a imagem $f(X)$ é um subgrupo do grupo (contradomínio) Y), aplicado ao homomorfismo de grupo $E_x : \mathbb{Z} \to G$, confirma que a imagem

$$\langle x \rangle = \{..., x^{-2}, x^{-1}, x^0 = e, x^1 = x, x^2, x^3, ...\}$$

E_x, o conjunto de todas as potências do elemento x, é realmente um subgrupo de G.
Dois casos a considerar:

- **Se** x **tem ordem infinita** o grupo núcleo de E_x é trivial. Assim E_x é injetiva e as potências

  $$..., x^{-2}, x^{-1}, x^0 = e, x^1 = x, x^2, x^3, ...$$

  de x são todas distintas. A parte (c) do primeiro teorema de isomorfismo para grupos (a bijeçã b), aplicado ao homomorfismo de grupo $E_x : \mathbb{Z} \to G$, surge o isomorfismo de grupo

  $$b : \mathbb{Z} \to \langle x \rangle;\ n \mapsto x^n$$

  entre o grupo cíclico infinito $\langle x \rangle$ e o grupo de inteiro $(\mathbb{Z}, +, 0)$ sob a multiplicação. Em geral, qualquer grupo C_∞ isomórfico ao grupo de inteiros é descrito como um *grupo cíclico infinito*.

- **Se** x **tem ordem finita** d_x, a bijeção b no primeiro teorema de isomorfismo para grupo mostra que x tem precisamente d_x potências distintas

  $$x^0 = e, x^1 = x, x^2, x^3, ..., x^{d_x - 1}.$$

  Como as classes da relação de núcleo $ker(E_x)$ são coclasses de subgrupos $d_x\mathbb{Z}$, duas potências x^m e x^n de x são iguais iff a diferença $m - n$ é um múltiplo de ordem d_x. Nesse caso, nós podemos também considerar os indeces n na potência x^n de x como inteiros módulo d_x. Em outras palavras, quando x tem ordem finita d, a bijeção b no primeiro teorema de isomorfismo para grupos surge o isomorfismo de grupo $b : \frac{\mathbb{Z}}{d} \to \langle x \rangle;\ n \mapsto x^n$ entre o grupo cíclico $\langle x \rangle$ de tamanha d e o grupo de inteiros $(\frac{\mathbb{Z}}{d}, +, 0)$ módulo d sob a operação de adição.

Em geral, qualquer grupo C_d isomórfico ao grupo dos inteiros módulo d sob a operação de adição é descrito como um *grupo cíclico* de ordem finita d.

Proposição 27
Seja x um elemento de um grupo G. Qualquer que seja a ordem de x (finita ou infinita), essa ordem é apenas o tamanho (ou a cardinalidade)

$$| \langle x \rangle |$$

do grupo cíclico $\langle x \rangle$ gerado por x.

Teorema de Cayley

Todo grupo é isomorfico a um grupo de permutações

Ora, para entendermos gradativamente iremos examinar semigrupos.
Seja $(S, \cdot)$ um semigrupo. Então para cada elemento s de S, nós definimos a *multiplicação a esquerda* por s sendo o mapa

$$\begin{aligned} \lambda_s : S &\to S \\ x &\mapsto s \cdot x. \end{aligned}$$

Exemplo 26 (Mudanças com reais)
Para cada real r defina a variação por r sendo o mapa

$$\sigma_r : \mathbb{R} \to \mathbb{R};\ x \mapsto r + x.$$

Note que para reais r, s e x temos

$$\sigma_r \circ \sigma_s(x) = r + (s + x) = (r + s) + x = \sigma_{r+s}(x),$$

assim $\sigma_r \circ \sigma_s = \sigma_{r+s}$.
Agora, seja $(R, +)$ o semigrupo dos números reais sob a operação de adição. Então, para cada número real r, a multiplicação a esquerda λ_r por r é a mudança σ_r.

Exemplo 27 (Os grupos cíclicos C_n)
Para cada inteiro positivo n, o grupo cíclico C_n consiste de n permutações

$$(0\ 1\ 2\ 3\ \ldots\ (n-2)\ (n-1)),$$

$$(0\ 1\ 2\ 3\ \ldots\ (n-2)\ (n-1))^2,$$

$$(0\ 1\ 2\ 3\ \ldots\ (n-2)\ (n-1))^3, \ldots$$

$$\ldots, (0\ (n-1)\ (n-2)\ \ldots\ 3\ 2\ 1),$$

e de (0) de S_n. Essas permutações correspondem a rotações antihorárias de um n-gon regular pelos ângulos

$$\frac{2\pi}{n}, 2\frac{2\pi}{n}, 3\frac{2\pi}{n}, \ldots, (n-1)\frac{2\pi}{n}, 0$$

radianos.
Agora, seja n um inteiro positivo. Seja $(\frac{\mathbb{Z}}{n}, +)$ um semigrupo de inteiros módulo n sob a operação de adição. Então λ_1 é o ciclo

$$(0\ 1\ 2\ \ldots\ (n-1))$$

do grupo cíclico C_n.

Proposição 28
Seja $(S, \cdot)$ um semigrupo. Considere o semigrupo $(S^S, \circ)$ de todas as funções do conjunto S nele mesmo, com a operação de composição de funções. Então o mapa

Demonstração. Para elementos s, t e x de S, a lei assosciativa surge

$$(\lambda_s \circ \lambda_t)(x) = \lambda_s(\lambda_t(x)) = \lambda_s(t \cdot x) = s \cdot (t \cdot x) = (s \cdot t) \cdot x = \lambda_{s \cdot t}(x).$$

Assim, o mapa composto $\lambda_s \circ \lambda_t$ é igual ao mapa singular $\lambda_{s \cdot t}$. Reescrevendo em termos de Λ, obtemos $\Lambda(s) \circ \Lambda(t) = \Lambda(s \cdot t)$, mostrando que Λ é um homomorfismo de semigrupo. ∎

Exemplo 28
Seja X um conjunto. Defina uma operação $*$ em X por

$$x * y = y,$$

$\forall, y \in X$. Essa operação é associativa, pois

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

$\forall x, y, z \in X$. No semigrupo $(X, \cdot)$, temos $\lambda_x = id_X$, $\forall x \in X$. O mapa Λ da proposição anterior se torna o mapa constante

$$\Lambda : x \mapsto id_x$$

nesse caso.

Para grupos, o colapso observado nesse exemplo anterior não pode acontecer. De fato, nós obtemos o isomorfismo desejado de cada grupo abstrato com um grupo de permutações.

Teorema 13 (TEOREMA DE CAYLEY)
Seja $(G, \cdot, e)$ um grupo.

(a) O homomorfismo de semigrupo

$$\Lambda : (G, \cdot) \to (G^G, \cdot);\ x \mapsto \lambda_x$$

é injetivo.

(b) A imagem de Λ é um grupo de permutações no conjunto G.

(c) O grupo abstrato G é isomorfico ao grupo $\Lambda(G)$ de permutações do conjunto G.

Demonstração. (a): Suponha $\lambda_x = \lambda_y$ para elementos x e y de G. Então

$$x = x \cdot e = \lambda_x(e) = \lambda_y(e) = y \cdot e = y.$$

(b): Para cada elemento x de G, o mapa λ_x é invertível, com inverso bilateral λ_{x-1}. De fato, para cada elemento g de G, temos

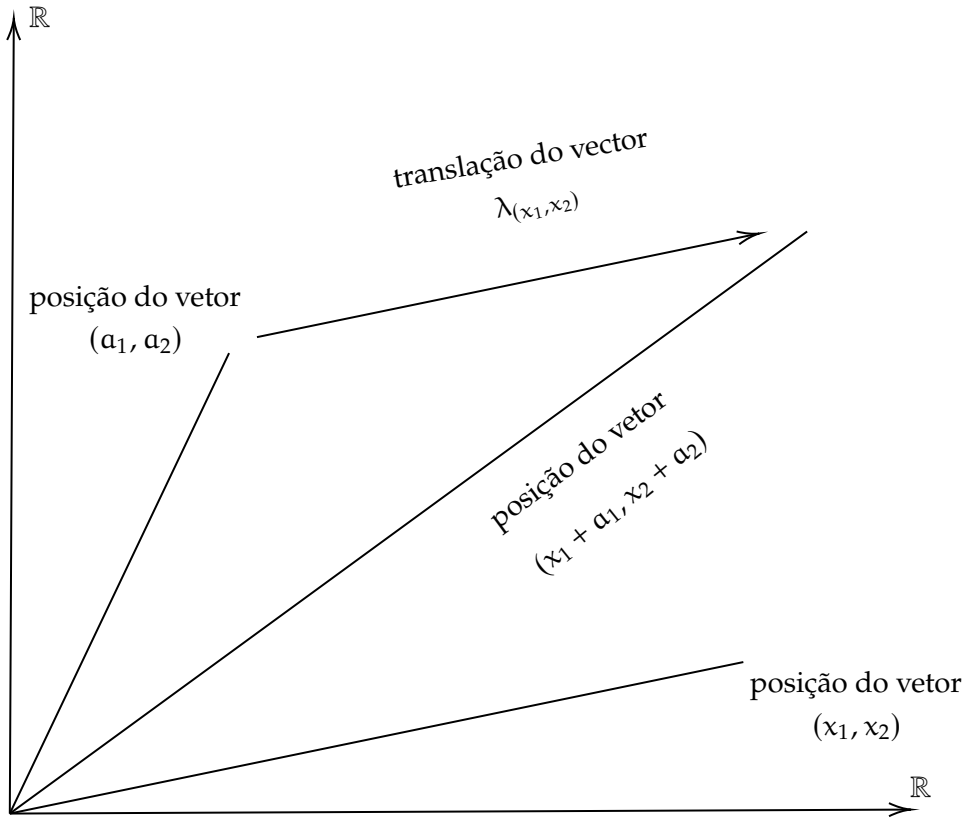
$$\lambda_x \circ \lambda_{x-1}(g) = x \cdot x^{-1} \cdot g = g = id_X(g),$$

assim $\lambda_x \circ \lambda_{x-1} = id_X$. Considerando x^{-1} no lugar de x surge $\lambda_{x-1} \circ \lambda_x = id_X$. (c): O mapa $(G, \cdot e) \to (\Lambda(G), \circ, id_X);\ x \mapsto \lambda_x$ é uma bijeção de homomorfismo de semigrupo entre grupos. Como visto antes, é um isomorfismo de grupo. ■

Exemplo 29 (Posição de vetores e translação de vetores)
Considere o grupo $\mathbb{R}^2$ de dimensão 2 dos vetores reais. Um elemento (x_1, x_2) de $\mathbb{R}^2$ representa a posição de um vetor. A imagem $\lambda_{(x_1,x_2)}$ em $\Lambda(\mathbb{R}^2)$ sob o teorema de isomorfismo (c) se torna a translação de vetor correspondente

$$\lambda_{(x_1,x_2)} :\ \mathbb{R}^2 \to \mathbb{R}^2;\ (a_1, a_2) \mapsto (x_1 + a_1, x_2 + a_2).$$

Assim, de acordo com o Teorema de Cayley, o grupo de posição de vetores sob a operação de adição é isomorfico ao grupo de translação de vetores sob a operação de adição.



Anéis

Os conjuntos mais conhecidos - como os dos inteiros $\mathbb{Z}$, os reais $\mathbb{R}$ ou as matrizes 2×2 reais $\mathbb{R}_2^2$ - carregam uma estrutura de grupo aditiva e uma estrutura de semigrupo multiplicativo (ou estrutura de monoide multiplicativo). Essas duas estruturas se combinam para formar uma estrutura mais rica conhecida como os anéis.

Definição de anel

Um anel é definido como um conjunto com duas operações, uma adição $x+y$ e uma multiplicação $x \cdot y$ (ou xy) de elementos x e y de R. A operação de multiplicação deve ser realizada primeiro. Dizemos que a multiplicação liga mais fortemente do que a adição.

Definição 29
Suponha que um conjunto R carrega uma estrutura de grupo aditiva comutativa $(R, +, 0)$ e uma estrutura de semigrupo multiplicativa $(R, \cdot)$.

(a) A estrutura combinada $(R, +, \cdot)$ diz-se que satisfaz a *lei distributiva a direita* se

$$(x + y) \cdot r = x \cdot r + y \cdot r, \qquad \forall x, y, r \in R. \tag{10}$$

(b) A estrutura $(R, +, \cdot)$ diz-se que satisfaz a *lei distributiva a esquerda* se

$$r \cdot (x + y) = r \cdot x + r \cdot y \qquad \forall x, y, r \in R. \tag{11}$$

(c) A estrutura $(R, +, \cdot)$ é dita ser um *anel não unitário* se satifazer ambas as leis (esquerda e direita) distributivas.

(d) Um anel $(R, +, \cdot)$ é dito ser um *anel unitário* se formar um monoide $(R, \cdot, 1)$ sob a operação de multiplicação.

(e) Um anel $(R, +, \cdot)$ é dito ser comutativo se o semigrupo $(R, \cdot)$ é comutativo.

Observações

- Note que a estrutura de grupo $(R, +, 0)$ de um anel $(R, +, \cdot)$ é sempre comutativa. O problema da comutatividade em um anel (item (e) da definição) surge apenas em conexão com a estrutura de semigrupo $(R, \cdot)$. Para um anel comutativo $(R, +, \cdot)$, a lei distributiva a esquerda e a direita coincidem. Em um anel geral $(R, +, \cdot)$, para dizer que dois elementos x e y comutam significa que $x \cdot y = y \cdot x$. O elemento identidade 0 do grupo aditivo $(R, +, 0)$ de um anel $(R, +, \cdot)$ é conhecido como o *zero* do anel R. Se R é unitário, então o elemento identidade 1 do monoide $(R, \cdot, 1)$ é conhecido como a *identidade* ou *um* do anel R. Anéis unitários são também descritos como *anéis com um*, não unitários são *anéis sem um*. Em um anel unitário R, os elementos invertíveis (unidades do monoide $(R, \cdot, 1)$) são chamados de *unidades* do anel R. O grupo de unidades de um anel unitário R é escrito como R^*.
- De acordo com a definição (item c), todos os anéis são não unitários, independentemente de possuírem ou não um elemento identidade. Quando um anel R do qual tem um elemento identidade é descrito como "não unitário"o elemento identidade está sendo desconsiderado.

Exemplo 30 (Inteiros)
Os inteiros formam um anel unitário comutativo $(\mathbb{Z}, +, \cdot)$ sob as operações triviais de adição e multiplicação. Note que a lei distributiva a direita

$$(m + n)r = mr + nr$$

reduz-se para a regra da potência no grupo aditivo $(\mathbb{Z}, +, 0)$.

Exemplo 31 (Reais)
O conjunto $\mathbb{R}$ dos números reais forma um anel unitário comutativo $(\mathbb{R}, +, \cdot)$ sob as operações triviais de adição e multiplicação.

Exemplo 32 (Anéis zero)
Seja $(A, +, 0)$ um grupo abeliano. Defina uma nova multiplicação trivial no conjunto A por

$$x \cdot_0 y = 0, \qquad \forall x, y \in A.$$

Então $(A, +, \cdot_0)$ é um anel não unitário comutativo conhecido como o *anel zero* no grupo abeliano $(A, +, \cdot)$. Note que as leis distributivas são satisfeitas trivialmente, pois cada lado das equações 10 e 11 em A vão para zero.

O exemplo a seguir mostra que mesmo tendo uma estrutura de grupo aditiva e uma estrutura de semigrupo conectada por uma das leis distributivas não é o suficiente para garantir que a outra lei distributiva será válida (para surgir um anel).

Exemplo 33
Seja $(A, +, 0)$ um grupo aditivo não trivial, com elemento a diferente de zero.
Define-se a operação de semigrupo

$$x \cdot y = y$$

em A. Note que a distributiva a esquerda é trivialmente válida, pois cada lado vai para

$$x + y.$$

Por outro lado, a distributiva a direita vai para

$$r = r + r,$$

da qual não é válida para $r = a$.

Exemplo 34 (O anel trivial)
O anel zero no grupo abeliano trivial $\{0\}$ é unitário, com 0 como o elemento identidade. Ele é conhecido como *anel trivial.*

Exemplo 35
Seja d um inteiro positivo. Então o conjunto $\frac{\mathbb{Z}}{d\mathbb{Z}}$ ou $\frac{\mathbb{Z}}{d}$ dos inteiros módulo d forma um anel unitário comutativo $(\frac{\mathbb{Z}}{d}, +, \cdot)$ sob as operações de adição modular e a multiplicação modular.4 Usando $[a]_{\mathrm{mod}\ d} + [b]_{\mathrm{mod}\ d} = [a + b]_{\mathrm{mod}\ d}$ e $[a]_{\mathrm{mod}\ d} \cdot [b]_{\mathrm{mod}\ d} = [a \cdot b]_{\mathrm{mod}\ d}$, a lei distributiva para $\frac{\mathbb{Z}}{d}$ segue da lei distributiva para inteiros. Note que para $d = 1$ o anel $\frac{\mathbb{Z}}{d}$ é o anel unitário zero de 34

Exemplo 36 (Anéis matrizes)
Para um anel não unitário R, deixe R_2^2 denotar o conjunto 2×2 das matrizes

$$\begin{bmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{bmatrix}$$

com entradas r_{ij} de R. Então R_2^2 forma um grupo comutativo aditivo sob a componente de adição, e um semigrupo não comutativo sob a operação trivial de multiplicação de matrizes. As leis distributivas também são válidas. Se o anel R é unitário, então também o é o anel de matriz R_2^2 correspondente. Seu elemento de identidade é a matriz

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

da qual as entradas são zero e a identidade do anel unitário R.

Exemplo 37 (Produto direto)
Seja $(R, +, \cdot)$ e $(S, +, \cdot)$ anéis não unitários. O grupo de produtos $(R \times S, +)$ e o semigrupo de produtos $(R \times S, \cdot)$ combinam para formar um anel $(R \times S, +, \cdot)$, o produto direto dos anéis R e S.
Note que as leis distributivas no produto segue a estrutura das leis distributivas nos fatores R e S. Se R e S são unitários, então $R \times S$ é unitário, com estrutura de elemento identidade $(1, 1)$.

Exemplo 38 (Anéis de Funções)
Sejam X um conjunto e $(S, +, \cdot)$ um anel. De acordo com a definição de estruturas de potência o conjunto S^X de todas as funções $f : X \to S$ de X para S carrega uma estrutura de grupo aditiva componente $(S^X, +, z)$ com a função constante zero

$$z : X \to S;\ x \mapsto 0$$

e a estrutura de semigrupo componente $(S^X, \cdot)$. Agora, para funções $f, g, h : X \to S$, a lei distributiva a direita em S implica

$$\begin{aligned}[(f + g) \cdot h](x) &= [f(x) + g(x)] \cdot h(x) \\ &= f(x) \cdot h(x) + g(x) \cdot h(x) = [f \cdot h + g \cdot h](x)\end{aligned}$$

para cada elemento x de X. Assim a lei distributiva a direita

$$(f + g) \cdot h = f \cdot h + g \cdot h$$

é válida em $(S^X, +, \cdot)$. Por um argumento similar a lei distributiva a esquerda também é válida. O conjunto S^X se torna um anel, a X-ésima potência do anel S, ou o anel de funções de S-valores no conjunto X. Se S é unitário, então também é potência S^X. É o elemento identidade a função $u : X \to S;\ x \mapsto 1$ da qual toma um valor constante da identidade em S a cada elemento x de X. Por exemplo o conjunto $\mathbb{R}^{\mathbb{R}}$ das funções reais $f : \mathbb{R} \to \mathbb{R}$ forma um anel unitário.

Distributividade em anéis

Vamos analisar um pouco a significância das leis de distributividade em um anel $(R, +, \cdot)$. Para um elemento r de R, considere a multiplicação a esquerda

$$R \to R;\ x \mapsto r \cdot x$$

por r. A lei distributiva a esquerda (da definição de anel) garante que a função acima é um homomorfismo de semigrupo de $(R, +)$ para ele mesmo. Isto é, $\exists \phi; \phi : (R, +) \to (R, +);\ x \mapsto x$. Pela proposição de homomorfismos de semigrupo entre grupos, seguimos que a multiplicação a esquerda por r é um homomorfismo de grupo de um grupo aditivo $(R, +, 0)$ de R para ele mesmo. Isto é, $\exists \varphi; \varphi : (R, +, 0) \to (R, +, 0);\ x \mapsto x$. Em outras palavras, a multiplicação perserva o zero e a negação:

$$r \cdot 0 = 0 \qquad \& \qquad r \cdot (-s) = -(rs)$$

para s em R. Ainda, temos

$$r \cdot (x - y) = r \cdot x - r \cdot y$$

para x e y em R.
Similarmente, a multiplicação a direita

$$R \to R;\ x \mapsto x \cdot s$$

por um elemento s de R é também um homomorfismo de grupo de $(R, +, 0)$ para ele mesmo. Assim

$$(-r) \cdot (-s) = r \cdot s$$

é válida para qualquer $r, s \in R$.
Outra propriedade útil é a equação

$$r \cdot 0 = 0 = 0 \cdot r, \qquad \forall r \in R.$$

De fato,

$$0 + r \cdot 0 = r \cdot 0 = r \cdot (0 + 0) = r \cdot 0 + r \cdot 0,$$

as primeiras duas equações são válidas pelos axiomas de grupo, e a terceira pela lei distributiva a esquerda. A cancelação no grupo $(R, +, 0)$ surge $0 = r \cdot 0$. A outra equação é provada similarmente.
Em um anel $(R, +, \cdot 0)$ é útil usar a notação sigma. Seja m um inteiro. Suponha que x_i é um elemento de R, para inteiros $i = m, m + 1, m + 2, \ldots$. Pela indução em n, define-se

$$\sum_{i=m}^{l} x_i = 0, \qquad \forall l < m$$

e

$$\sum_{i=m}^{n+1} x_i = x_{n+1} + \sum_{i=m}^{n} x_i.$$

Assim, por exemplo,

$$\sum_{i=1}^{5} x_i = x_1 + x_2 + x_3 + x_4 + x_5.$$

Usando a notação sigma nós formulamos uma extensão das leis distributivas, que pode ser provada por indução.

Proposição 29 (Lei distributiva generalizada)
Seja x_i e y_i elementos de um anel R, para $i = 1, 2, 3, \ldots$. Então

$$\left(\sum_{i=1}^{m} x_i\right) \cdot \left(\sum_{j=1}^{n} y_j\right) = \sum_{i=1}^{m} \sum_{j=1}^{n} x_i y_j, \qquad m, n \in \mathbb{N}.$$

Corolário 13.1
Seja x e y elementos de um anel $(R, +, \cdot)$. Então para inteiros m e n,

$$(mx) \cdot (ny) = (mn)xy.$$

Demonstração. A prova se divide naturalmente em 4 casos:

- Para $m, n > 0$, coloque $x_i = x$ e $y_j = y$ na proposição anterior.
- Para $m < 0$, $n > 0$, coloque $x_i = -x$ e $y_j = y$ na proposição anterior.
- Para $m > 0$, $n < 0$, coloque $x_i = x$ e $y_j = y$ na proposição anterior.
- Para $m, n < 0$, coloque $x_i = -x$ e $y_j = -y$ na proposição anterior.

■

Subanéis

Aqui iremos combinar conceitos de subsemigrupos, submonoides e subsemigrupos para o conceito de um subanel de um anel.

Definição 30 (ANÉIS UNITÁRIOS E NÃO UNITÁRIOS)
.

(a) Um subconjunto S de um anel não unitário $(R, +, \cdot)$ é dito ser um subanel não unitário de R se S é um subgrupo de $(R, +, 0)$ e um subsemigrupo de $(R, \cdot)$.

(b) Um subconjunto S de um anel unitário $(R, +, \cdot)$ é dito ser um *subanel unitário* de R se S é um subgrupo de $(R, +, 0)$ e um submonoide de $(R, \cdot, 1)$.

Isto é, para termos um subanel S basta que S seja fechado para a diferença e para o produto.
Com efeito:

$$\begin{aligned} S &\neq \varnothing \\ a - b &\in S \\ a \cdot b &\in S \end{aligned}$$

Observações

As vezes é deixa implícito se um subanel é declarado unitário ou não unitário.

- Em qualquer anel R, o subconjunto R forma ele próprio um subanel, o **subanel impróprio**.
- Sempre será um subanel não unitário.
- Se R é unitário, então terá um subanel unitário.
- O anel $\{0\}$ e o próprio R são triviais.
- O anel $\{0\}$ é um subanel não unitário para cada anel R.

Exemplo 39
$\mathbb{Z}$ é um subanel de $\mathbb{Q}$ com unidade

Exemplo 40
$2\mathbb{Z}$ é um subanel de $\mathbb{Z}$. Lembrando que $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ é o conjunto dos números pares. Neste caso, $2\mathbb{Z}$ é um anel sem unidade. Isto é, $1 \notin 2\mathbb{Z}$.

Exemplo 41
$d\mathbb{Z}$ é um subanel de $\mathbb{Z}$. Claro que $d\mathbb{Z} = \{dk \mid k \in \mathbb{Z}\}$, n inteiro e $n > 1$, é o conjunto dos múltiplos de n. Assim, $n\mathbb{Z}$ também é um anel sem unidade ($1 \notin n\mathbb{Z}$).

Exemplo 42
Como visto antes, cada subgrupo do grupo aditivo $(\mathbb{Z}, +, 0)$ dos inteiros é o conjunto $d\mathbb{Z}$ dos múltiplos de algum número natural d. Como a relação de divisibilidade é transitiva, cada subgrupo de $(\mathbb{Z}, +, 0)$ é também um subsemigrupo de $(\mathbb{Z}, \cdot)$, e então um subanel não unitário do anel unitário dos inteiros. De fato, como $1\mathbb{Z} = \mathbb{Z}$, o único subanel unitário de $\mathbb{Z}$ é o subanel impróprio.

Exemplo 43 (O anel Ri, Números Complexos, Inteiros Gaussianos)
Seja R um anel unitário, e seja $R[i]$ o conjunto das matrizes 2×2 da forma

$$\begin{bmatrix} x & -y \\ y & x \end{bmatrix}$$

para $x, y \in R$. Então $R[i]$ é um subanel unitário do anel R_2^2 de todas as matrizes 2×2 sob R. Certamente a matriz identidade I_2 está em $R[i]$, e $R[i]$ é fechado sob a componente de subtração das matrizes. Agora

$$\begin{bmatrix} x & -y \\ y & x \end{bmatrix}\begin{bmatrix} u & -v \\ v & u \end{bmatrix} = \begin{bmatrix} xu - yv & -xv - yu \\ yu + xv & -yv + xu \end{bmatrix} = \begin{bmatrix} (xu - yv) & -(yu + xv) \\ (yu + xv) & (xu - yv) \end{bmatrix} \tag{12}$$

de modo que $R[i]$ também é **fechado** sob a multiplicação. Se R é comutativo, segue de 43 que $R[i]$ também é comutativo. Aqui nós temos dois casos especiais:

- O Anel $\mathbb{R}[i]$ é o anel $\mathbb{C}$ dos números complexos.
- O Subanel $\mathbb{Z}[i]$ de $\mathbb{R}[i]$ é conhecido como o anel dos Inteiros Gaussianos.

Referências

[1] Israel Nathan Herstein. *Abstract Algebra*. 3ª ed. Wiley, 1996. ISBN: 978-0471368793.

[2] Jonathan D. H. Smith. *Introduction to Abstract Algebra*. 1ª ed. Chapman e Hall/CRC, 2009. ISBN: 978-1-4200-6371-4, 1420063715.

[3] Arnaldo Garcia; Yves Lequain. *Elementos de Álgebra*. 6ª ed. IMPA, 2018. ISBN: 978-85-244-0450-4.