Universidade Federal do Rio de Janeiro
Instituto de Matemática

Notas em Algebra

Douglas Vieira
dvieira@disroot.org

10/2021

Conteúdo

Introdução

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.

Mapas

Primeiro, um exemplo de mapa: 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.

Definição 1. O mapeamento $f : S \to T$ é sobrejetivo se cada $t \in T$ é a imagem sob f de algum $s \in S$; isto é, *iff*, dado $t \in T$, existe um $s \in S$ tal que $t = f(s)$.

Maneiras para dizer que um mapeamento $f : S \to T$ é sobrejetivo:

$$f(S) = \{f(s) \in T \mid s \in S\}$$

$$f(S) = T.$$

Definição 2. Um mapeamento $f : S \to T$ é injetivo se para $s_1 \neq s_2$ em S, $f(s_1) \neq f(s_2)$ em T. Equivalentemente, f é um mapa um-para-um (1-1) se $f(s_1) = f(s_2)$ implica que $s_1 = s_2$.

Parafraseando, temos que um mapa injetivo é aquele que pega elementos distintos para imagens distintas.
Há diversos casos onde f^{-1} não define um mapeamento de T para S por certos motivos.
Primeiro, se f não é sobrejetiva, então existe algum t em T para o qual não é imagem de nenhum elemento s, então $f^{-1}(t) = \emptyset$.
Segundo, se f não é injetiva, então para algum $t \in T$ existem ao menos dois distintos $s_1 \neq s_2$ em S tal que $f(s_1) = t = f(s_2)$. Então $f^{-1}(t)$ não é um único elemento de S, algo que nós precisamos em nossa definição de mapeamento. Agora, sendo injetivo e sobrejetivo você pode verificar que f^{-1} define um meapeamento de T em S.

Definição 3. O mapeamento $f : S \to T$ é bijetivo se f é injetivo e sobrejetivo.

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

Lema 1. Se $f : S \to T$ é uma bijeção, então $f \circ f^{-1} = i_T$ e $f^{-1} \circ f = i_S$, onde i_S e i_T são as identidades dos mapeamentos de S e de T, respectivamente.

Demonstração. Primeiramente, temos $(f \circ f^{-1})(t) = f(f^{-1}(t))$. Pela definição, f^{-1} é o elemento $s_0 \in S$ tal que $t = f(s_0)$. Então $f(f^{-1}(t)) = f(s_0) = t$. Ora, isso significa que $(f \circ f^{-1})(t) = t$, validando a identidade deste mapeamento em T. ■

Para $f^{-1} \circ f = i_S$ funciona analogamento como para i_T

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 2. $A(S)$ 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 $n(n-1)(n-2)\cdots 1 = n!$. O contexto disso é que queremos enviar um elemento s em n maneiras dentro do próprio S.

Exemplo 1. 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. $f \circ f : s_1 \to s_3; s_2 \to s_1; s_3 \to s_2$.

Definição 4. 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 3. 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, $f \circ (g \circ h) = (f \circ g) \circ h$. ■

Inteiros

Definição 5 (Princípio da boa-ordenação)**.** Qualquer conjunto não vazio de inteiros não negativos possui um elemento pequeno.

$$S \neq \emptyset, S \in \mathbb{Z}_+, s_0 \in S : s_0 \leq S, \forall s \in S.$$

Teorema 4 (Algoritmo de Euclides)**.**

$$m = qn + r$$

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

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

Definição 6. $m, n \in \mathbb{Z}, m \neq 0$, dizemos que m divide n, ou m é divisor de n

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

Definição 7. 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 5. Se a, b são inteiros não negativos, 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 8. 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 5.1. Os inteiros a e b são primos relativos *iff* $1 = ma + nb$, para m e n adequados.

Teorema 6. Se a e b são primos relativos e $a \mid bc$, então $a \mid c$.

Demonstração. Pelo colorário 5.1, $ma + nb = 1$ 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 9. 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 7. Se p é um primo e $p \mid (a_1 a_2 a_3 \cdots a_n)$, então $p \mid a_i$ para algum i com $1 \leq i \leq n$.

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 $p \mid a_1(a_2 a_3 \cdots a_n)$, então pelo teorema 6, $p \mid (a_2 a_3 \cdots a_n)$. 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 8. 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 5), 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 9. Dado $n > 1$, então existe uma e somente uma maneira de escrever n na forma $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, onde $p_1 < p_2 < \ldots < p_k$ são primos e os expoentes $a_1, a_2, \ldots a_k$ 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 $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = q_1^{b_1} q_2^{b_2} \cdots q_l^{b_l}$ onde $p_1 < p_2 < \ldots < p_k$, $q_1 < q_2 < \ldots < q_l$ são primos e onde os expoentes $a_1, \ldots, a_k$ e $b_1, \ldots, b_l$ são todos positivos. Sendo $p_1 \mid p_1^{a_1} \cdots p_k^{a_k} = q_1^{b_1} \cdots q_l^{b_l}$, pelo teorema 7 $p_1 \mid q_i^{b_1}$ para algum i; assim, também pelo teorema 7 $p_1 \mid q_i$, temos $p_1 = q_i$. Pela mesma razão $q_1 = p_j$ para algum j; assim $p_1 \leq p_j = q_1 \leq q_i = p_1$. 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 $\frac{m}{p_1} = p_1^{a_1 - 1} p_2^{a_2} \cdots p_k^{a_k} = q_1^{b_1 - 1} q_2^{b_2} \cdots q_l^{b_l}$ 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 expoentes 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 10. 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 $q = 1 + p_1 p_2 \cdots p_k$. 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 8 , 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 11. 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 $k \geq 1$, então $P(k + 1)$ também é verdadeiro. (*passo indutivo*)

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