Estruturas Algébricas

Aula 2

Os Inteiros

Abramo Hefez

2025

O conjunto $\mathbb{Z}$ dos inteiros é um anel muito especial que possui uma série de propriedades adicionais que o caracterizam completamente. Isso significa que qualquer outro anel possuindo essas mesmas propriedades é "essencialmente" o anel $\mathbb{Z}$. Para dar sentido a essas áspas, vamos introduzir no que se segue um conceito fundamental.

Homomorfismos

O poder de abstração da Álgebra reside em podermos identificar objetos com a mesma estrutura algébrica que são essencialmente os mesmos, apesar de serem apresentados com distintas roupagens. Para isto, precisamos definir as *funcões naturais* em cada contexto.

No contexto dos anéis essas funções são os **homomorfismos de anéis**.

Dados dois anéis A e B, uma função $h\colon A \to B$ será chamada *homomorfismo* de A em B, se valerem as seguintes propriedades:

Para todos $a, b \in A$, tem-se que

$$\begin{aligned} &h(a+b) = h(a) + h(b), \\ &h(a \cdot b) = h(a) \cdot h(b) \\ &h(1) = 1 \end{aligned}$$

onde as operações nos primeiros membros dessas igualdades são realizadas em A, enquanto que as dos segundos membros são realizadas em B.

Um **isomorfismo de anéis** é um homomorfismo bijetor. Dois anéis serão ditos *isomorfos* se existir um isomorfismo entre eles. Nesse caso, escrevemos $A \simeq B$.

Do ponto de vista das estruturas algébricas, dois anéis isomorfos são considerados para todos os efeitos "iguais".

Proposição Se $h\colon A \to B$ é um homomorfismo de anéis, então:

i) $h(0) = 0$;

ii) Quaisquer que sejam $a, b \in A$, temos que $h(a - b) = h(a) - h(b)$. Em particular, $h(-a) = -h(a)$;

iii) $h(A)$ é um subanel de B;

iv) Se h é bijetora, então $h^{-1}\colon B \to A$ é um homomorfismo de anéis.

Demonstração. (i) Note que

$$h(0) = h(0 + 0) = h(0) + h(0).$$

Logo somando $-h(0)$ a ambos os lados da igualdade acima, temos que $h(0) = 0$.

(ii) Observe inicialmente que

$$0 = h(0) = h(a + (-a)) = h(a) + h(-a),$$

logo $h(-a) = -h(a)$. Agora

$$h(a - b) = h(a + (-b)) = h(a) + h(-b) = h(a) - h(b).$$

(iii) De (i) temos que $0 \in h(A)$ e da definição, $1 = h(1) \in h(A)$. Que somas e produtos de elementos de $h(A)$ estão em $h(A)$, seguem-se das condições (1) e (2) da definição de homomorfismo. Que o simétrico de um elemento de $h(A)$ está em $h(A)$, decorre de (ii).

(iv) Suponha h bijetora e sejam $y, y' \in B$. Logo existem $x, x' \in A$, univocamente determinados, tais que $h(x) = y$ e $h(x') = y'$. Temos, então que

$$\begin{aligned} h^{-1}(y + y') = \quad h^{-1}(h(x) + h(x')) = & \quad h^{-1}(h(x + x')) = \\ x + x' = & \quad h^{-1}(y) + h^{-1}(y'). \end{aligned}$$

Temos também que

$$\begin{aligned} h^{-1}(y \cdot y') = \quad h^{-1}(h(x) \cdot h(x')) = & \quad h^{-1}(h(x \cdot x')) = \\ x \cdot x' = & \quad h^{-1}(y) \cdot h^{-1}(y'). \end{aligned}$$

Finalmente, é claro que $h^{-1}(1) = 1$.

Exemplo Se $X = \{x_1, \ldots, x_n\}$ é um conjunto finito com n elementos e A é um anel, então temos que $\mathcal{F}(X, A) \simeq A^n$.
De fato, considere a função

$$\begin{array}{rccc} h\colon & \mathcal{F}(X, A) & \to & A^n \\ & f & \mapsto & (f(x_1), \ldots, f(x_n)) \end{array}$$

Vamos provar que h é um isomorfismo de anéis.

Como uma função é determinada pelos valores que assume nos elementos do domínio, temos que h é bijetora.

Vejamos agora as outras propriedades que definem um homomorfismo.

$$\begin{aligned} h(f+g) &= ((f+g)(x_1), \ldots, (f+g)(x_n)) \\ &= (f(x_1)+g(x_1), \ldots, f(x_n)+g(x_n)) \\ &= (f(x_1), \ldots, f(x_n)) + (g(x_1), \ldots, g(x_n)) \\ &= h(f)+h(g), \end{aligned}$$

$$\begin{aligned} h(f \cdot g) &= ((f \cdot g)(x_1), \ldots, (f \cdot g)(x_n)) \\ &= (f(x_1) \cdot g(x_1), \ldots, f(x_n) \cdot g(x_n)) \\ &= (f(x_1), \ldots, f(x_n)) \cdot (g(x_1), \ldots, g(x_n)) \\ &= h(f) \cdot h(g) \end{aligned}$$

Definindo $\mathbf{1} \colon X \to A$, por $\mathbf{1}(x_i) = 1$, para todo $i = 1, \ldots, n$, que é o elemento neutro para a multiplicação de $\mathcal{F}(X, A)$, temos que

$$h(\mathbf{1}) = (\mathbf{1}(x_1) \ldots, \mathbf{1}(x_n)) = (1, \ldots, 1),$$

de modo que h leva o elemento neutro da multiplicação de $\mathcal{F}(X, A)$ no elemento neutro de A^n.

Os Inteiros

O que torna o anel dos inteiros único?

Nesta aula introduziremos as propriedades que caracterizam univocamente o anel dos inteiros dentre os demais anéis.

Ordenação

O conjunto dos inteiros possui uma ordenação devido ao fato de termos um subconjunto distinguido de $\mathbb{Z}$ que é o conjunto dos *números naturais*

$$\mathbb{N} = \{1, 2, 3, \ldots\},$$

fechado para a adição e para a multiplicação.

Com esse subconjunto obtemos a seguinte partição de $\mathbb{Z}$:

$$\mathbb{Z} = -\mathbb{N} \cup \{0\} \cup \mathbb{N},$$

onde $-\mathbb{N} = \{-1, -2, -3, \ldots\}$.

Os elementos de $\mathbb{N}$ serão chamados de inteiros positivos, enquanto que os de $-\mathbb{N}$ são chamados de inteiros negativos.

A ordenação nos inteiros é dada pela relação:

$$a \leq b \iff b - a \in \mathbb{N} \cup \{0\},$$

que será lida a **é menor ou igual** a b.

Se $a \leq b$, escreveremos também $b \geq a$, que se lê b **maior ou igual** a a.

No caso em que $b - a \in \mathbb{N}$, escreveremos $a < b$, ou $b > a$, o que se lê a é **menor** do que b, ou b é **maior** do que a, respectivamente.

A relação $\leq$ é uma **relação de ordem**, isto é, possui as seguintes propriedades:

Reflexividade: $a \leq a$, para todo $a \in \mathbb{Z}$;

Antissimetria: Se $a \leq b$ e $b \leq a$, então $a = b$;

Transitividade Se $a \leq b$ e $b \leq c$, então $a \leq c$.

Essa relação de ordem é compatível com as operações de adição e de multiplicação de $\mathbb{Z}$:

Compatibilidade com a adição: $\forall a, b, c \in \mathbb{Z}$, Se $a \leq b$, então $a + c \leq b + c$;

Compatibilidade com a multiplicação: $\forall a, b, c \in \mathbb{Z}$, com $0 \leq c$, se $a \leq b$, então $ac \leq bc$.

Além disso, possui a seguinte propriedade adicional:

Totalidade: Quaisquer que sejam $a, b \in \mathbb{Z}$, tem-se que uma das três condições é satisfeita $a < b$, $a = b$, ou $b < a$.

Se um anel A possui uma relação de ordem compatível com as operações, como acima, dizemos que é um **anel ordenado**. Se a relação de ordem for *total*, isto é, se possuir adicionalmente a propriedade de totalidade, dizemos que o anel é **totalmente ordenado**.

Por exemplo, $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ são anéis totalmente ordenados.

Existem anéis que não são totalmente ordenados, como podemos ver no próximo exemplo:

Exemplo O anel $\mathbb{C}$ não é totalmente ordenado.

De fato, em um anel totalmente ordenado A, é fácil verificar que $a^2 \geq 0$ para todo $a \in A$ e que $-1 < 0$.

Suponhamos por absurdo que $\mathbb{C}$ seja um anel totalmente ordenado.

Então $0 \leq i^2 = -1 < 0$, o que é uma contradição.

Em um anel totalmente ordenado, define-se o **valor absoluto** de um elemento $a \in A$ como sendo,

$$|a| = \begin{cases} a & , \quad \text{se } a \geq 0 \\ -a & , \quad \text{se } a < 0 \end{cases}$$

Decorre imediatamente dessa definição que $|a| \geq 0$, para todo $a \in A$, valendo a igualdade se, e somente se, $a = 0$.

Proposição Se A é um anel totalmente ordenado e $a, b, r \in A$, com $r \geq 0$, então:

i) $|a \cdot b| = |a| \cdot |b|$;

ii) $-|a| \leq a \leq |a|$;

iii) $|a| \leq r$ *se, e somente se,* $-r \leq a \leq r$;

iv) $\big|\,|a| - |b|\,\big| \leq |a \pm b| \leq |a| + |b|$.

Prova A prova é idêntica à que se faz em Cálculo I.

Boa ordenação

As propriedades acima listadas dos inteiros não são suficientes para caracterizá-los.

Por exemplo, além de $\mathbb{Z}$, os anéis $\mathbb{Q}$ e $\mathbb{R}$ possuem as referidas propriedades.

Há porém mais uma propriedade que o anel dos inteiros possui que o distingue dos demais anéis, que é a propriedade da **boa ordenação** que passamos a detalhar.

Seja dado um anel totalmente ordenado A. Um subconjunto não vazio C de A será dito **limitado inferiormente**, se existir um elemento $\alpha \in A$ tal que $\alpha \leq c$, para todo $c \in C$.

Diremos que o conjunto C tem um **menor elemento**, quando existir $a \in C$ tal que $a \leq c$, para todo $c \in C$.

Axioma da boa ordenação dos inteiros (PBO): Todo subconjunto não vazio de $\mathbb{Z}$ limitado inferiormente possui um menor elemento.

Um anel satisfazendo ao Axioma da Boa Ordenação, é dito um **anel bem ordenado**.

Os anéis $\mathbb{Q}$ e $\mathbb{R}$ não são bem ordenados, pois os conjuntos $\{x \in \mathbb{Q};\ x > 0\}$ e $\{x \in \mathbb{R};\ x > 0\}$ são limitados inferiormente, mas não possuem um menor elemento.

Os anéis bem ordenados possuem uma propriedade fundamental, que é óbvia nos inteiros.

Proposição Seja A um anel bem ordenado e seja $a \in A$. Se $a > 0$, então $a \geq 1$.

Prova Suponha por absurdo que exista $a \in A$ tal que $0 < a < 1$.

Logo o conjunto

$$S = \{x \in A;\ 0 < x < 1\}$$

é não vazio e limitado inferiormente.

Portanto, S possui um menor elemento b tal que $0 < b < 1$.

Segue-se então que $0 < b^2 < b < 1$ e, consequentemente, $b^2 \in S$ e $b^2 < b$, absurdo.

Corolário Sejam A um anel bem ordenado e $a, b \in A$. Se $a > b$, então $a \geq b + 1$.

Prova Aplique a proposição com $a - b$ no lugar de a.

Assim, em um anel bem ordenado, $\forall a \in A$, entre a e $a + 1$ não existem elementos de A.

Veremos daqui a pouco que, a menos de isomorfismo que respeita as ordens, $\mathbb{Z}$ é o único anel bem ordenado.

Portanto, esse conjunto de propriedades:
ser um anel totalmente ordenado, e
ser bem ordenado
caracterizarão completamente o anel dos inteiros com a sua ordenação.

Corolário Sejam A um domínio bem ordenado e $a, b \in A$, com $b \neq 0$. Então $|a \cdot b| \geq |a|$.

Prova Como $b \neq 0$, temos que $|b| \geq 1$. Multiplicando ambos os membros desta desigualdade por $|a|$, segue-se que

$$|a \cdot b| = |a| \cdot |b| \geq |a|.$$

Princípio de Indução Matemática

Uma das consequências da propriedade de boa ordenação dos inteiros é um importante método para demonstrar resultados em matemática.

Teorema(Princípio de Indução Matemática) Seja $P(n)$ uma sentença aberta em $\{n \in \mathbb{Z}\,;\; n \geq n_0\}$, tal que

i) $P(n_0)$ é verdade.

ii) Para todo $n \geq n_0$, se $P(n)$ é verdade, então $P(n+1)$ é verdade.

Então $P(n)$ é verdade para todo $n \geq n_0$.

Prova Seja $F = \{n \in \mathbb{Z};\ n \geq n_0 \text{ e } P(n) \text{ é falso}\}$. Queremos provar que F é vazio.

Suponha, por absurdo, que $F \neq \emptyset$. Como F é limitado inferiormente (por n_0), pelo Princípio da Boa Ordenação, temos que F possui um menor elemento b.

Como $b \in F$, temos que $b \geq n_0$, mas, por (i), temos que $n_0 \notin F$, logo $b \neq n_0$ e, portanto, $b > n_0$.

Sendo b o menor elemento de F, temos que $b - 1 \notin F$, logo $P(b-1)$ é verdade.

De (ii), segue-se, então, que $P(b)$ é verdade e, portanto, $b \notin F$, contradição.

Na realidade, o Princípio da Boa Ordenação é equivalente ao Princípio de Indução Matemática, fato que será assunto de um problema da Lista 2 de exercícios.

O Princípio de Indução Matemática permite definir objetos matemáticos recorrentemente como segue:

Para definir uma expressão $E(n)$ para todo $n \in \mathbb{Z}$, $n \geq a$, basta definirmos $E(a)$ e mostrar como obter $E(n+1)$ a partir de $E(n)$, para todo $n \in \mathbb{Z}$, com $n \geq a$.

Exemplo(definição do fatorial) Seja $n \in \mathbb{N}$, define-se

$$n! = \begin{cases} 1 & \text{se } n = 1 \\ n(n-1)! & \text{se } n \geq 2 \end{cases}$$

Define-se adicionalmente $0! = 1$.

Dado um anel A, podemos definir o "produto" de um elemento $a \in A$ por um número inteiro $n \in \mathbb{Z}$, como segue:

$$na = \begin{cases} 0 & , \quad \text{se} \quad n = 0 \\ a + (n-1)a & , \quad \text{se} \quad n \geq 1 \\ -((-n)a) & , \quad \text{se} \quad n < 0 \end{cases}$$

Proposição Para todo $a \in A$ e todos $m, n \in \mathbb{Z}$, temos

i) 1a=a;

ii) $m(a + b) = ma + mb$;

iii) $m(a \cdot b) = (ma) \cdot b$;

iv) $(m + n)a = ma + na$;

v) $(mn)a = m(na)$;

vi) $(-m)a = -(ma)$.

(iii) e (v) implicam que $ma \cdot nb = mn(a \cdot b)$.

A demonstração desses fatos pode ser feita sem dificuldade utilizando o Princípio de Indução Matemática e é deixada como exercício

Das propriedades acima, segue-se que a aplicação natural

$$\begin{aligned} \rho\colon \mathbb{Z} &\longrightarrow A \\ n &\longmapsto n1 \end{aligned}$$

é um homomorfismo de anéis, chamado de **homomorfismo característico**.

De fato, $\rho(n+m) = (n+m)1 = n1 + m1 = \rho(n) + \rho(m)$,
$\rho(nm) = (nm)1 = n1 \cdot m1 = \rho(n) \cdot \rho(m)$,
$\rho(1) = 11 = 1$.

Portanto, qualquer que seja o anel comutativo A existe um homomorfismo ρ de $\mathbb{Z}$ em A.

O resultado a seguir nos garantirá que esse é o único homomorfismo possível de $\mathbb{Z}$ em um anel comutativo A, chamado de **homomorfismo característico**. Neste preciso sentido é que $\mathbb{Z}$ é considerado um "objeto inicial na categoria dos anéis".

Proposição Se $h\colon \mathbb{Z} \to A$ é um homomorfismo de anéis, então $h = \rho$.

Prova Note que, sendo h um homomorfismo de anéis, temos que $h(0) = \rho(0) = 0$.

Vamos provar, por indução sobre n, que para todo $n \geq 0$ temos

$$h(n) = n1 \ (= \rho(n)). \tag{1}$$

Suponha que para algum $n \geq 0$, a igualdade (1) seja verificada, logo

$$h(n+1) = h(n) + h(1) = n1 + 1 = (n+1)1 = \rho(n+1),$$

o que demonstra a igualdade (1) para todo $n \geq 0$.

Por outro lado, pelo caso $n \geq 0$ que acabamos de provar, temos que se $n < 0$, então

$$h(n) = -h(-n) = -(-n)1 = n1 = \rho(n).$$

Com isto acabamos de provar que

$$h(n) = \rho(n), \quad \forall\, n \in \mathbb{Z}.$$

Proposição Se A é um anel ordenado, então ρ é um homomorfismo injetor de anéis ordenados.

Prova Inicialmente provaremos por indução que se $n \in \mathbb{Z}$, com $n > 0$, então $n1 > 0$.

Para $n = 1$, isto é claro já que em qualquer anel ordenado temos $1 > 0$ (pois $1 = 1^2 > 0$).

Suponha agora que para um dado $n > 0$ tenhamos $n1 > 0$.

Somando $1 \in A$ a ambos os membros dessa desigualdade, temos

$$(n + 1)1 = n1 + 1 > 0,$$

obtendo $(n + 1)1 > 0$.

Consequentemente, para todo $n > 0$, temos que $n1 > 0$. Disto decorre que se $n < 0$, então $n1 < 0$.

Suponha que $m < n$, logo $n - m > 0$ e, portanto, $(n - m)1 > 0$, obtendo
$$\rho(n) - \rho(m) = n1 - m1 = (n - m)1 > 0.$$
Logo, $\rho(m) < \rho(n)$. Isto mostra que ρ é um homomorfismo injetor de anéis ordenados.

Teorema Se A é um domínio bem ordenado, então ρ é um isomorfismo de anéis ordenados.

Prova Sabemos que ρ é um homomorfismo injetor de anéis ordenados.

Falta apenas provar que ρ é sobrejetor, o que equivale a mostrar que todo elemento $a \in A$ é da forma $n1$ para algum $n \in \mathbb{Z}$.

Suponha por absurdo que exista $a \in A$ tal que $n1 \neq a$ para todo $n \in \mathbb{Z}$. Considere os seguintes subconjuntos de A:

$$S_1 = \{n1\,;\; n \in \mathbb{Z} \;\text{ e }\; n1 > a\} \quad \mathrm{e} \quad S_2 = \{n1\,;\; n \in \mathbb{Z} \;\text{ e }\; n1 < a\}.$$

Mostraremos que $S_1 = S_2 = \emptyset$, o que é uma contradição.

Suponha que $S_1 \neq \emptyset$. Sendo S_1 limitado inferiormente, pelo Princípio da Boa Ordenação, ele possui um menor elemento $m1$, logo $m1 > a$ e $(m-1)1 \leq a$.

Como $(m-1)1 \neq a$ (pela nossa hipótese sobre a), temos que $(m-1)1 < a$ e, consequentemente, temos que

$$m1 = (m-1)1 + 1 \leq a, \qquad \text{contradição.}$$

De modo análogo, prova-se que $S_2 = \emptyset$, usando, porém, a formulação equivalente do Princípio da Boa Ordenação:

PBO' Todo conjunto limitado superiormente possui um maior elemento.

O teorema acima nos garante que:

A menos de isomorfismo ordenado, $\mathbb{Z}$ é o único anel bem ordenado.

FIM DA AULA 2