Estruturas Algébricas

Estruturas Algébricas

Alessandra Negrini Dalla Barba

Dados Internacionais de Catalogação na Publicação (CIP)

Dalla Barba, Alessandra Negrini
D144e Estruturas algébricas / Alessandra Negrini Dalla Barba.
– Londrina : Editora e Distribuidora Educacional S.A., 2018.
224 p.

ISBN 978-85-522-1119-8

1. Estruturas algébricas. 2. Álgebra.I. Dalla Barba, Alessandra Negrini. II. Título.

CDD 512.55

Thamiris Mantovani CRB-8/9491

2018
Editora e Distribuidora Educacional S.A.
Avenida Paris, 675 – Parque Residencial João Piza
CEP: 86041-100 — Londrina — PR
e-mail: editora.educacional@kroton.com.br
Homepage: http://www.kroton.com.br/

Sumário

Palavras do autor

Seja bem-vindo ao estudo das Estruturas Algébricas! Uma das grandes áreas da Matemática é a Álgebra, cujos conhecimentos possibilitaram a representação de relações por meio da articulação entre valores numéricos e literais, favorecendo, dentre outros, a representação de fenômenos por meio das equações algébricas.

O estudo da Álgebra tem início na Educação Básica, no entanto, vai além da abordagem das equações algébricas, pois um de seus grandes temas de estudo são as estruturas algébricas, essenciais para a formalização dos conjuntos com operações e propriedades associadas. As estruturas algébricas foram desenvolvidas ao longo do processo de axiomatização da Álgebra, principalmente na estruturação de operações associadas a conjuntos e, mais especificamente, os numéricos. A partir dessa introdução, diversos conhecimentos da Álgebra podem ser abordados, como as propriedades das operações definidas sobre os conjuntos numéricos empregadas na resolução, por exemplo, de equações de 1º grau.

O conhecimento dessas estruturas é essencial para que o professor de Matemática possa abordar os temas direcionados à Educação Básica de forma adequada, atendendo às especificidades das etapas correspondentes. Assim, neste livro didático, abordaremos algumas das principais estruturas algébricas: os grupos, os anéis e os corpos, suas propriedades e os principais conceitos associados, observando a aplicabilidade destes na resolução de problemas, favorecendo o desenvolvimento do raciocínio crítico e da persistência.

Tendo em vista a organização desses conceitos, este livro foi sistematizado em quatro unidades. Na Unidade 1 daremos início aos estudos a respeito das estruturas algébricas, analisando tópicos da Teoria dos Conjuntos e da Teoria dos Números, os quais comporão as definições das estruturas algébricas. Na sequência, na Unidade 2, iniciaremos os estudos específicos a respeito das estruturas algébricas a partir da definição de grupo, observando os principais conceitos associados, tais como propriedades, grupos abelianos, principais exemplos e subgrupos. Na Unidade 3, daremos continuidade ao estudo das estruturas algébricas com os anéis, com base nos grupos abordados na unidade anterior, observando suas

propriedades, características, categorias e exemplos importantes. Na Unidade 4, finalizaremos os estudos com a definição de corpo, relacionando-a aos anéis, identificando suas propriedades, analisando os polinômios e os anéis correspondentes, os domínios euclidianos, homomorfismos e isomorfismos de anéis.

Para favorecer o aprendizado, procure organizar uma rotina de estudos realizando a pré-aula e a pós-aula correspondentes. Estude também os demais materiais sugeridos ao longo deste livro para complementar os tópicos da Álgebra abordados. Procure identificar os conceitos principais discutidos em cada unidade, estabelecendo relações entre estes e observando sua aplicabilidade na resolução dos problemas propostos.

Tendo em vista os objetivos e conteúdos associados, vamos iniciar esse novo desafio, investigando as estruturas algébricas, suas principais características e aplicações!

Teoria dos Números

Convite ao estudo

Seja bem-vindo à Unidade 1 deste livro. No decorrer desta unidade discutiremos a respeito de conceitos importantes da Álgebra Abstrata, principalmente em relação à Teoria dos Números e à Teoria de Conjuntos.

O estudo de tópicos da Álgebra Abstrata é essencial para o desenvolvimento de conceitos da Matemática, o que por sua vez possibilita a investigação e a resolução de problemas das mais variadas áreas nas quais a Matemática pode ser aplicada, como a avaliação de dados coletados a partir de pesquisas, a modelagem de fenômenos a partir de equações polinomiais, entre outros. O conhecimento a respeito dos conjuntos, suas relações e operações são essenciais para todo professor de Matemática, pois, além de serem abordados na Educação Básica, fundamentam outras ideias, como o conceito de função.

Para motivar sua aprendizagem, considere que você faz parte do quadro de funcionários de um escritório que atua no ramo de consultoria e que presta serviços para companhias de diversas áreas. Nesse escritório você é responsável por uma equipe que atua com ações, por exemplo, a realização de pesquisas de opinião, análises estatísticas, estudo da inteligência de mercado, entre outros.

Uma empresa que trabalha com construção civil entrou em contato com o escritório no qual você atua solicitando uma consultoria referente ao setor imobiliário. Nessa tarefa, sua equipe precisará realizar análise de dados relacionados ao interesse das pessoas a respeito dos tipos de imóveis e propor formas de organização das numerações de imóveis em condomínios, empregando as propriedades dos conjuntos numéricos para a resolução dos problemas propostos.

Considerando o contexto apresentado, sua primeira tarefa consiste em conhecer as preferências de compradores em potencial a respeito das quantidades de quartos dos apartamentos a serem construídos pela empresa. Em seguida, você precisará capacitar os funcionários recém-contratados pela empresa para integrar sua equipe a respeito das operações binárias e suas principais propriedades, pois esses conceitos são essenciais para o desenvolvimento da terceira tarefa, a qual consiste em construir uma estratégia para identificação das numerações das casas de um novo empreendimento a ser lançado pela empresa.

Que conhecimentos matemáticos são necessários para o estudo destes problemas? De que forma você poderá executar essas tarefas? Prossiga com a leitura e verifique o primeiro problema que deve ser solucionado.

Seção 1.1

A Álgebra Abstrata e a Teoria de Conjuntos

Diálogo aberto

Nesta seção abordaremos os principais tópicos da Teoria dos Conjuntos, visando o estudo dos conjuntos, suas relações e operações correspondentes, conceitos que serão utilizados posteriormente na definição das estruturas algébricas. Na Educação Básica, esses conceitos são tratados considerando suas adequações à etapa considerada, porém, é preciso que o professor tenha o conhecimento teórico correspondente para que possa desenvolver tarefas significativas aos alunos e auxiliá-los na superação de suas dificuldades.

Considerando a sua função enquanto chefe de equipe no escritório de consultoria, o primeiro problema que deverá ser resolvido pelo seu setor diz respeito à análise de dados relacionados ao ramo imobiliário.

A empresa de construção civil que contatou o escritório no qual você trabalha pretende iniciar um novo projeto com a construção de um edifício residencial. Porém, antes de finalizar o projeto desse novo empreendimento, a empresa deseja conhecer quais são as preferências dos compradores em potencial em relação às quantidades de quartos que cada apartamento deve conter dentre as seguintes possibilidades: um, dois ou três quartos.

Para isso, o escritório em que você trabalha organizou e realizou uma pesquisa com o público alvo, conforme o perfil da empresa, e coletou alguns dados a respeito das preferências deste. Com a realização da pesquisa, dentre as 450 pessoas entrevistadas, foram obtidas as seguintes respostas:

- 160 pessoas preferem apartamentos com um quarto.
- 231 pessoas preferem apartamentos com dois quartos.
- 182 pessoas preferem apartamentos com três quartos.
- 33 pessoas preferem apartamentos com um ou dois quartos apenas.

- 57 pessoas preferem apartamentos com um ou três quartos.
- 65 pessoas preferem apartamentos com dois ou três quartos.
- 25 pessoas não possuem uma preferência específica, afirmando que as três opções as agradam.
- 32 pessoas não souberam opinar.

A sua equipe ficou responsável por analisar estes dados e apresentar respostas aos seguintes questionamentos: quantas pessoas preferem apartamentos com apenas dois quartos? Qual a porcentagem de pessoas, em relação ao total, que preferem apenas apartamentos com dois ou três quartos? Qual seria a melhor opção para a empresa: construir um edifício com apartamentos de um, dois ou três quartos?

Após analisar os dados coletados, buscando respostas para os questionamentos apresentados pela empresa, você e sua equipe devem construir um relatório que será entregue às partes interessadas com as análises realizadas a partir do conjunto de dados em questão, empregando diferentes recursos para evidenciar as relações observadas, como a construção de gráficos e tabelas envolvendo os dados coletados e analisados, por exemplo.

Como você pode orientar sua equipe neste estudo e quais seriam as melhores respostas a cada um dos questionamentos apresentados pela empresa? Prossiga em seus estudos para identificar os conhecimentos necessários para a resolução desse problema.

Não pode faltar

Introdução ao estudo da Álgebra Abstrata

Atualmente, a Álgebra pode ser dividida em dois grupos: a Álgebra Elementar, cujos estudos são voltados, dentre outros, às equações e métodos de resoluções; e a Álgebra Abstrata, a qual trata a respeito das estruturas matemáticas, tais como grupos, anéis e corpos. Para que a Álgebra atingisse o formato atual, ao longo da história foram necessários muitos estudos e evoluções, partindo inicialmente do uso de diálogos na descrição dos conteúdos, empregando resumos e abreviações em uma fase intermediária para, assim, finalizar com a construção de um sistema eficiente de representação simbólica, processos que favoreceram o desenvolvimento da estrutura atual empregada para a apresentação dos conhecimentos da Álgebra.

Pesquise mais

Para mais informações a respeito das origens históricas da Álgebra, consulte a seção intitulada "A álgebra de Al-Khwarizmi", localizada no capítulo 4 do livro "História da Matemática", de autoria de Tatiana Roque. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788537809099>. Acesso em: 16 mar. 2018. Realize o login em sua biblioteca virtual para que possa acessar o material indicado por meio do link apresentado.

Ao longo desse livro trataremos a respeito de tópicos da Álgebra Abstrata, principalmente em relação às estruturas algébricas: grupos, anéis e corpos, bem como suas propriedades características. Porém, para que possamos estudar essas estruturas, precisaremos de conceitos relativos à Teoria dos Conjuntos e Teoria dos Números, pois estes estarão presentes, dentre outros, na construção das estruturas algébricas e na identificação de suas principais propriedades.

Nesse sentido, daremos início aos trabalhos a partir de tópicos da Teoria dos Conjuntos.

Reflita

Com base nos conhecimentos de outras áreas, como a Língua Portuguesa ou a Biologia, quais são exemplos de conjuntos que podem ser estudados?

Estudo dos conjuntos e suas representações

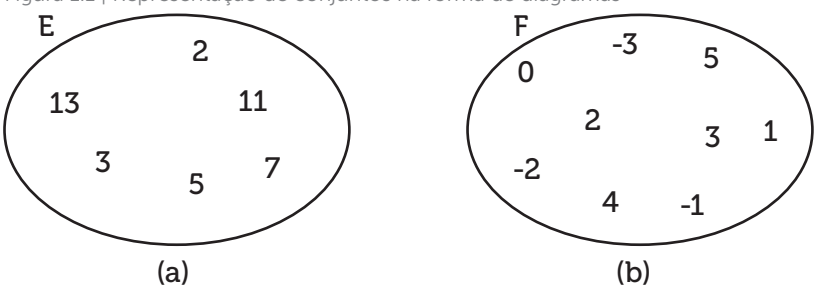
Em relação à Teoria de Conjuntos, o conceito inicial que precisa ser estudado é o de conjunto, bem como suas principais representações.

Um **conjunto** corresponde a uma coleção qualquer de números, objetos, figuras geométricas, entre outros, desde que todos os elementos envolvidos possuam algum tipo de semelhança entre si. **Elemento** pode ser entendido como um integrante de um conjunto.

Podemos adotar como notação para os conjuntos as letras maiúsculas do alfabeto. Em relação à **representação**, podemos adotar três formas distintas, descritas a seguir:

- 1ª forma: enumerar os elementos do conjunto, escrevendo-os entre chaves e separados por vírgulas, conforme os exemplos apresentados a seguir:
  - $A = \{1, 2, 3, 4, 5\}$, que corresponde ao conjunto composto pelos números naturais 1, 2, 3, 4 e 5;
  - $B = \{1, 2, 3, 4, 6, 12\}$, que se refere ao conjunto formado pelos números naturais que são divisores de 12.
- 2ª forma: identificar uma propriedade que caracteriza os elementos dos conjuntos, por exemplo:
  - $C = \{x \mid x \text{ é um número inteiro par}\}$, ou seja, o conjunto $C = \{..., -4, -2, 0, 2, ...\}$;
  - $D = \{y \mid y \text{ é a solução da equação } y + 2 = 0\}$, e nesse caso, $D = \{-2\}$.
- 3ª forma: empregando a representação em diagramas, conforme os seguintes exemplos:
  - Conjunto E composto pelos números primos entre 2 e 13, com o acréscimo do 2 e do 13, o qual é ilustrado na Figura 1.1(a);
  - Conjunto F composto pelos números inteiros entre -3 e 5, com a inclusão destes, destacado na Figura 1.1(b).

Figura 1.1 | Representação de conjuntos na forma de diagramas



Fonte: elaborado pelo autor.

Assimile

Os integrantes de um conjunto são elementos e as possíveis representações para os conjuntos são: enumeração de seus elementos; e identificação de propriedade dos elementos que o compõem e diagramas.

Faça você mesmo

Analise os conjuntos apresentados a seguir e enumere seus elementos a partir da propriedade indicada:

- $M = \{x \mid x \text{ é um número natural divisor de } 24\}$;
- $N = \{y \mid y \text{ é solução da equação } y^2 - 2y - 3 = 0\}$;
- $P = \{z \mid z \text{ é raiz da função } f(z) = z^2 - 7z + 10\}$.

Relações de pertinência e inclusão envolvendo conjuntos

Podemos avaliar as relações entre elementos e conjuntos por meio da pertinência e da inclusão, conceitos que se diferem pela natureza dos objetos a serem comparados.

Dizemos que um elemento x **pertence** a um conjunto A quando x faz parte do conjunto em estudo e, quando isso ocorre, podemos utilizar a notação $x \in A$ (lê-se "x pertence a *A*"). Por outro lado, quando x não pertence ao conjunto, empregamos a notação $x \notin A$ (lê-se "x não pertence a *A*"). Assim, a pertinência permite relacionar elementos e conjuntos.

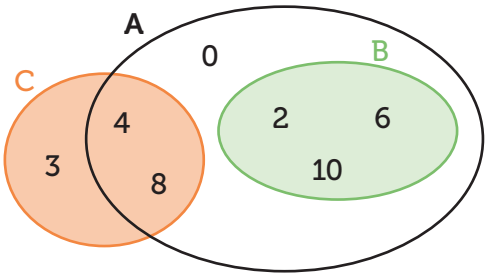
Por exemplo, podemos afirmar que o número 2 pertence ao conjunto $S = \{1,2,3,4,5,...\}$ dos inteiros positivos, mas -3 não pertence a S. No caso do conjunto $R = \{...,-6,-3,\ 0,\ 3,\ 6,...\}$ dos inteiros múltiplos de 3, podemos afirmar que $9 \in R$ enquanto que $2 \notin R$.

A inclusão possibilita relacionar diferentes conjuntos entre si, mais especificamente quando desejamos verificar se um conjunto contém outro conjunto. Dizemos que um conjunto *B* está **contido** no conjunto *A* quando todo elemento de *B* também for elemento de *A* e, nesse caso, utilizamos as notações $B \subset A$ (lê-se "*B* está contido em *A*") ou $A \supset B$ (lê-se "*A* contém *B*"), e no caso contrário, temos a notação $B \not\subset A$ (lê-se "*B* não está contido em *A*") ou $A \not\supset B$ (lê-se "*A* não contém *B*").

Como exemplo, podemos tomar os conjuntos $A = \{0,\ 2,\ 4,\ 6,\ 8,\ 10\}$, $B = \{2,\ 6,\ 10\}$ e $C = \{3,\ 4,\ 8\}$. Note que $B \subset A$ (ou $A \supset B$) porque todos os elementos de *B* também pertencem ao conjunto *A*. Porém, o conjunto *C* não está contido

em *A*, isto é, $C \not\subset A$ (ou $A \not\supset C$), porque $3 \in C$ mas $3 \notin A$. Essas relações são ilustradas na forma de diagramas conforme a Figura 1.2.

Figura 1.2 | Relações entre os conjuntos *A*, *B* e *C*



Fonte: elaborado pelo autor.

Sendo assim, a pertinência permite que relacionemos elementos a conjuntos, sendo representada pelos símbolos $\in$ e $\notin$, enquanto que a relação de inclusão refere-se à comparação entre conjuntos, a qual pode ser representada por $\subset$ e $\not\subset$. Desta forma, temos diferenças entre os dois conceitos, suas representações e os termos que devem ser empregados em cada situação.

A partir da relação de inclusão podemos estudar os subconjuntos. Se *B* está contido no conjunto *A* então dizemos que *B* é um **subconjunto** de *A*.

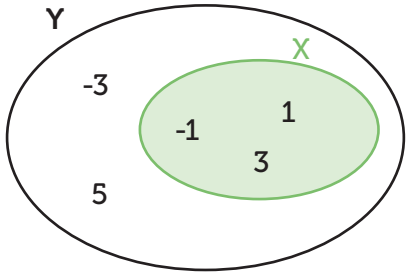
Reflita

Considerando a relação de inclusão, por que podemos afirmar que qualquer conjunto é subconjunto dele mesmo? Como podemos justificar esse fato?

Exemplificando

Considere os conjuntos $X = \{-1, 1, 3\}$ e $Y = \{-3, -1, 1, 3, 5\}$. Note que o conjunto *X* está contido em *Y*, ou $X \subset Y$, pois todo elemento de *X* também pertence a *Y*, então *X* é um subconjunto de *Y*. A relação de inclusão entre os conjuntos *X* e *Y* é ilustrada na Figura 1.3 na forma de diagrama.

Figura 1.3 | Relação de inclusão entre X e Y



Fonte: elaborado pelo autor.

Na Figura 1.3 podemos observar que *X* é um subconjunto de *Y* e, além disso, os elementos -3 e 5 são elementos de *Y* que não pertencem ao conjunto *X*. Assim, a partir desse exemplo, podemos definir o complementar de um conjunto.

Tomando dois conjuntos *A* e *B* tais que $B \subset A$, o **complementar** do conjunto *B* em relação ao *A* corresponde ao conjunto formado por todos os elementos de *A* que não pertencem a *B*. Essa relação pode ser representada por $\left(B^c\right)_A = \{x \in A \mid x \notin B\}$. No caso do exemplo relativo à Figura 1.3, temos $X \subset Y$ e $\left(X^c\right)_Y = \{x \in Y \mid x \notin X\} = \{-3,\ 5\}$.

Considerando as características das relações de pertinência e de inclusão, podemos afirmar que dois conjuntos *A* e *B* são **iguais** quando possuem exatamente os mesmos elementos, situação que pode ser denotada por $A = B$ (lê-se "*A* é igual a *B*"). Quando ocorre a igualdade entre os conjuntos *A* e *B*, pela relação de inclusão podemos afirmar que $A \subset B$ e $B \subset A$. Em resumo, dois conjuntos *A* e *B* são iguais se, e somente se, $A \subset B$ e $B \subset A$.

Alguns conjuntos particulares que podem ser estudados são os unitários, vazios e das partes.

- **Conjunto unitário**: conjunto que contém um único elemento, por exemplo, o conjunto P que contém apenas o número 2, isto é, $P = \{2\}$.
- **Conjunto vazio**: conjunto que não contém elemento algum, denotado por $\{\ \}$ ou $\varnothing$.

Reflita

Uma característica particular do conjunto vazio é de que o mesmo está contido em todos os conjuntos, isto é, $\varnothing$ é subconjunto de qualquer conjunto. Como podemos justificar este fato?

- **Conjunto das partes**: conjunto *P(X)*, relativo a outro conjunto *X*, e que contém todos os subconjuntos que podem ser construídos a partir dos elementos de *X*, inclusive o conjunto vazio. Assim, se $X = \{1, 3, 5\}$, o conjunto das partes associados a *X* será dado por $P(X) = \{\varnothing, \{1\}, \{3\}, \{5\}, \{1,3\}, \{1,5\}, \{3,5\}, \{1,3,5\}\}$. Se o conjunto *X* contém n elementos, então a quantidade de elementos do conjunto das partes *P(X)* será igual a 2^n elementos.

Faça você mesmo

Determine o conjunto das partes associado ao conjunto $T = \{2, 5, 7, 9\}$.

Operações envolvendo conjuntos

Além de relacionar os conjuntos a partir das ideias de pertinência e inclusão, podemos também estabelecer operações envolvendo conjuntos, dentre as quais podemos destacar a união, a interseção e a diferença.

Sejam os conjuntos *A* e *B* dados. Definimos a **união** entre os conjuntos *A* e *B*, denotada por $A \cup B$, como o conjunto formado pelos elementos que pertencem ao conjunto *A* ou ao conjunto *B*, a qual pode ser descrita da seguinte forma:

$$A \cup B = \{x \mid x \in A \text{ ou } x \in B\}$$

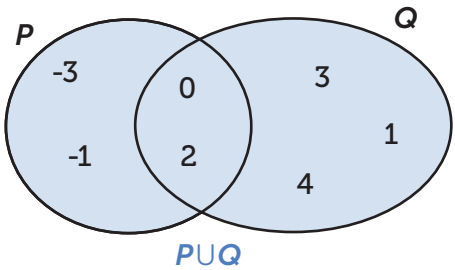
Exemplificando

Sejam os conjuntos $P = \{-3, -1, 0, 2\}$ e $Q = \{0, 1, 2, 3, 4\}$. A união dos conjuntos *P* e *Q*, isto é, $P \cup Q$, corresponde ao conjunto

$$P \cup Q = \{-3, -1, 0, 1, 2, 3, 4\}$$

A representação na forma de diagramas é dada na Figura 1.4.

Figura 1.4 | União dos conjuntos *P* e *Q*



Fonte: elaborado pelo autor.

Sendo assim, na união não existe a exclusão de elementos dos conjuntos envolvidos, pois desde que o elemento pertença a pelo menos um dos conjuntos considerados ele pertencerá à união.

Assimile

Sendo *A*, *B* e *C* conjuntos quaisquer, a operação de união entre conjuntos satisfaz as seguintes propriedades:

- Reflexiva: $A \cup A = A$;
- Comutativa: $A \cup B = B \cup A$;
- Associativa: $A \cup (B \cup C) = (A \cup B) \cup C$;
- Elemento neutro para a união: $A \cup \varnothing = A$;
- Inclusão relacionada: se $B \subset A$ então $A \cup B = A$.

Como essas propriedades podem ser demonstradas? Que argumentos são necessários? Reflita a respeito dessas propriedades, identificando justificativas adequadas para cada uma delas.

Pesquise mais

As propriedades referentes à união de conjuntos devem ser demonstradas com base em argumentos válidos. Para verificar as demonstrações para algumas dessas propriedades, consulte o material Conjuntos.

Disponível em: <https://www.math.tecnico.ulisboa.pt/~fteix/CI/conjuntos.pdf>. Acesso em: 2 abr. 2018. As demonstrações são construídas, nesse material, a partir de argumentos e conceitos provenientes da Lógica.

Considerando os conjuntos A e B dados, podemos definir a **interseção** entre os conjuntos A e B, denotada por <<u1s1Eqn065.eps>>, como o conjunto formado pelos elementos que pertencem ao conjunto A e ao conjunto B, a qual pode ser descrita da seguinte forma:

$$A \cap B = \{x \mid x \in A \text{ e } x \in B\}.$$

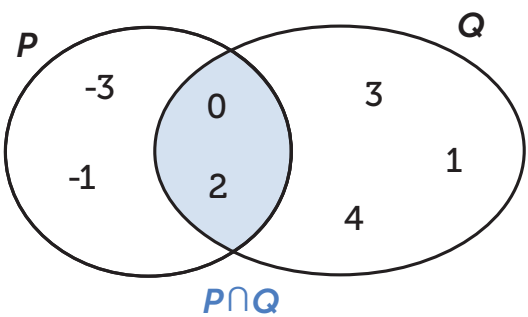
Exemplificando

Sejam os conjuntos $P = \{-3, -1, 0, 2\}$ e $Q = \{0, 1, 2, 3, 4\}$. A interseção dos conjuntos P e Q, isto é, $P \cap Q$, corresponde ao conjunto

$$P \cap Q = \{0, 2\}$$

A representação na forma de diagramas é dada na Figura 1.5.

Figura 1.5 | Interseção dos conjuntos P e Q



Fonte: elaborada pelo autor.

Desta forma, diferente da união, os elementos que não pertencem a todos os conjuntos envolvidos são excluídos do conjunto interseção.

Assimile

Sendo *A*, *B* e *C* conjuntos quaisquer, a operação de interseção entre conjuntos goza das seguintes propriedades:

- Reflexiva: $A \cap A = A$;
- Comutativa: $A \cap B = B \cap A$;
- Associativa: $A \cap (B \cap C) = (A \cap B) \cap C$;
- Elemento neutro para a interseção: $A \cap \varnothing = \varnothing$;
- Inclusão relacionada: se $B \subset A$ então $A \cap B = B$.

Como proposta de estudo complementar, construa argumentos de modo a demonstrar a validade de cada uma das propriedades apresentadas.

Podemos ainda estudar, além da união e interseção, a diferença entre conjuntos.

Sejam conjuntos *A* e *B*. A **diferença** entre *A* e *B* corresponde aos elementos que pertencem ao conjunto *A* e que não pertencem a *B*, a qual pode ser descrita por $A - B = \{x \mid x \in A \text{ e } x \notin B\}$. Por exemplo, considerando os conjuntos $K = \{1, 4, 7, 10, 15\}$ e $L\{1, 3, 4, 6\}$ então $K - L = \{7, 10, 15\}$.

A diferença entre conjuntos satisfaz às seguintes propriedades para quaisquer conjuntos *A* e *B*:

- $A - A = \varnothing$;
- $A - \varnothing = A$;
- $\varnothing - A = \varnothing$;
- Se $B \subset A$ então $B - A = \varnothing$.

Reflita também a respeito dessas propriedades, construindo demonstrações que justifiquem a validade de cada uma.

Faça você mesmo

Avalie os conjuntos apresentados a seguir e determine as diferenças $D - E$, $E - F$ e $F - D$:

$D = \{1, 2, 3, 4, 7\}$, $E = \{-4, 0, 4, 7, 8\}$, $F = \{-4, 4, 8\}$.

Pesquise mais

Para contribuir com os estudos a respeito da Teoria de Conjuntos, inclusive a respeito das operações e relações correspondentes, consulte o material a seguir.

Disponível em: <http://www.uel.br/projetos/matessencial/medio/conjuntos/conjunto.htm>. Acesso em: 11 abr. 2018.

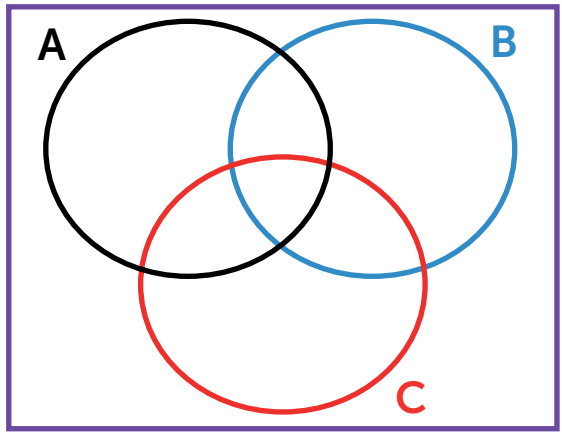
Não pode faltar

No contexto de atuação no escritório de consultoria, a tarefa a ser cumprida por você e sua equipe consiste na avaliação das preferências de compradores em potencial em relação às quantidades de quartos que apartamentos devem conter dentre as possibilidades: um, dois ou três quartos.

Para o estudo desse problema, sejam os seguintes conjuntos: conjunto *A*, composto pelas pessoas que preferem apartamentos com um quarto; conjunto *B*, das que preferem apartamentos com dois quartos; e conjunto *C*, das que preferem apartamentos com três quartos. Assim, é necessário analisar os dados coletados pelo escritório em relação aos 450 entrevistados.

Este problema envolve três conjuntos, os quais podem possuir interseções entre si. Isso ocorre devido ao fato de que algumas pessoas podem preferir, por exemplo, apartamentos com dois ou três quartos e, assim, estas serão contadas tanto no conjunto *B* quanto no *C*. Esse fato pode ser confirmado devido à soma das quantidades de elementos dos conjuntos *A*, *B* e *C* ser igual a 573 e superar o total de 450 entrevistados, logo, existem pessoas que foram contabilizadas em mais de uma categoria. Os conjuntos relacionados ao problema podem ser estudados a partir de diagramas, conforme exemplo apresentado na Figura 1.6.

Figura 1.6 | Diagramas representando os conjuntos *A*, *B* e *C* e possíveis interseções



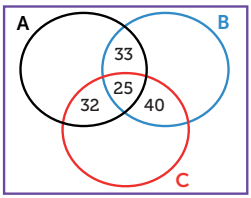
Fonte: elaborada pelo autor.

Para auxiliar na interpretação dos dados, podemos preencher os diagramas da Figura 1.6 com as quantidades de pessoas associadas a cada conjunto e suas possíveis interseções.

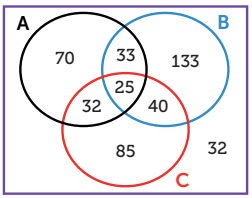
Em relação às interseções, cujo diagrama é apresentado na Figura 1.7(a), temos os casos:

- 25 pessoas não possuem uma preferência específica, afirmando que as três opções as agradam, logo, o conjunto $A \cap B \cap C$ contém 25 elementos.
- 33 pessoas preferem apartamentos com um ou dois quartos apenas, então o conjunto $(A \cap B) - C$ contém 33 elementos.
- 57 pessoas preferem apartamentos com um ou três quartos, e $57 - 25 = 32$ preferem apartamentos com um ou três quartos apenas, o que corresponde a $(A \cap C) - B$.
- Das 65 pessoas que preferem apartamentos com dois ou três quartos, $65 - 25 = 40$ preferem apartamentos com dois ou três quartos apenas, referente a $(B \cap C) - A$.

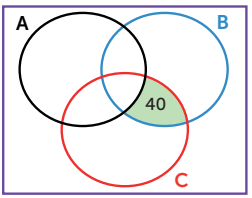
Figura 1.7 | Diagrama de *A*, *B* e *C* com as quantidades de elementos correspondentes



(a) Interseções



(b) Diagramas completos

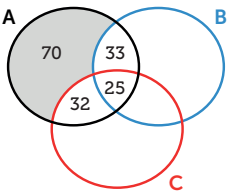


(c) Conjunto (B ∩ C) – A

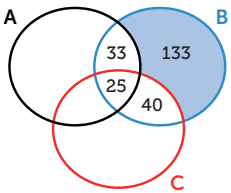
Fonte: elaborada pelo autor.

Para as quantidades de elementos associados a apenas um dos três conjuntos, visando a construção do diagrama da Figura 1.7(b), temos, das 160 pessoas que preferem apartamentos com um quarto, $33+25+32=90$ pessoas que já foram consideradas nas interseções. Logo, $160-90=70$ pessoas preferem apartamentos com um quarto apenas (conjunto $A-(B\cup C)$), fato evidenciado na Figura 1.8(a). Para os outros dois conjuntos, de modo análogo, obtemos que $231-(33+25+40)=133$ pessoas preferem apartamentos com dois quartos apenas (conjunto $B-(A\cup C)$), conforme Figura 1.8(b), e $182-(32+25+40)=85$ pessoas preferem apartamentos com três quartos apenas (conjunto $C-(A\cup B)$), como a Figura 1.8(c).

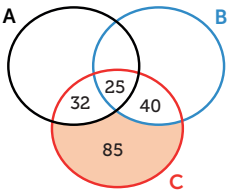
Figura 1.8 | Diagramas para $A-(B\cup C)$, $B-(A\cup C)$ e $C-(A\cup B)$



(a) Conjunto *A* — (*B*∪*C*)



(b) Conjunto *B* — (*A*∪*C*)



(c) Conjunto *C* — (*A*∪*B*)

Fonte: elaborada pelo autor.

Do total, 32 não souberam opinar, os quais não pertencem aos diagramas associados aos conjuntos *A*, *B* e *C*, então obtemos o diagrama da Figura 1.7(b). Dessa figura é possível constatar que 133 pessoas preferem apartamentos com apenas dois quartos (conjunto $B-(A\cup C)$).

As 40 pessoas que preferem apartamentos com dois ou três quartos apenas compõem o conjunto $(B \cap C) - A$, destacado na Figura 1.7(c). Se a quantidade total de pessoas é 450, as 40 pessoas correspondem a $\frac{40}{450} \cong 0.089 = 8.9\%$ do total de entrevistados.

Dos totais de pessoas que preferem apenas apartamentos com um, dois ou três quartos, a maior quantidade corresponde aos de dois quartos (conjunto B). Considerando os dados coletados e que todos os apartamentos do edifício apresentarão as mesmas quantidades de cômodos, a melhor opção para a empresa seria um edifício com apartamentos de dois quartos apenas.

Após esses estudos, você deverá elaborar um relatório contemplando um resumo dos dados coletados e analisados a respeito do problema proposto. Organize as informações obtidas a partir de gráficos e tabelas, buscando evidenciar para a empresa quais são as preferências do público pesquisado a respeito das quantidades de quartos que os apartamentos deveriam conter.

Avançando na prática

Investigação das propriedades referentes às operações entre conjuntos

Descrição da situação-problema

Durante a elaboração de um plano de aula voltado ao estudo da união e interseção envolvendo conjuntos no Ensino Médio, você deparou-se com a seguinte afirmação:

Propriedade: Se A, B e C são conjuntos quaisquer então a seguinte igualdade é válida:

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$$

A partir de estudos de tópicos da Álgebra, você sabe que esta propriedade pode ser aplicada na resolução de problemas práticos, no entanto, é preciso demonstrá-la para garantir a validade das conclusões obtidas a partir dela.

Nesse sentido, de modo a aprofundar os estudos a respeito das demonstrações empregadas no estudo da Álgebra, e sabendo que é válida a relação

$X = Y$ se, e somente se, $X \subset Y$ e $Y \subset X$

para quaisquer conjuntos *X* e *Y*, prove que a propriedade em questão é válida com base nas definições das operações de união e interseção de conjuntos.

Resolução da situação-problema

Para demonstrar que a igualdade $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ é válida para conjuntos *A*, *B* e *C* quaisquer, precisamos comprovar a validade das seguintes inclusões:

$(A \cup B) \cap C \subset (A \cap C) \cup (B \cap C)$ (1)

$(A \cap C) \cup (B \cap C) \subset (A \cup B) \cap C$ (2)

Segue a demonstração da inclusão (1): Seja $x \in (A \cup B) \cap C$, sendo assim, pela definição da interseção de conjuntos, $x \in A \cup B$ e $x \in C$. Da relação $x \in A \cup B$ e pela definição da união de conjuntos temos que $x \in A$ ou $x \in B$. Consequentemente, uma das seguintes situações será verdadeira:

- $x \in A$ e $x \in C$, isto é, $x \in A \cap C$; ou
- $x \in B$ e $x \in C$, ou ainda, $x \in B \cap C$.

Como uma das possibilidades deve ocorrer, então devemos ter $x \in (A \cap C) \cup (B \cap C)$, de acordo com a definição da união de conjuntos. Logo, $(A \cup B) \cap C \subset (A \cap C) \cup (B \cap C)$, o que conclui a demonstração da primeira relação de inclusão.

A seguir temos a demonstração da inclusão (2): Considere $y \in (A \cap C) \cup (B \cap C)$, o que pela definição da união entre conjuntos implica em $y \in A \cap C$ ou $y \in B \cap C$. Pela definição de interseção, do primeiro caso segue que $y \in A$ e $y \in C$ e, sendo y um elemento de A, temos também que $y \in A \cup B$, de acordo com as propriedades da união de conjuntos, pois $A \subset A \cup B$. De modo análogo, no segundo caso temos $y \in B$ e $y \in C$, o que implica em $y \in A \cup B$ e $y \in C$, pois $B \subset A \cup B$. Sendo assim, em ambas as situações temos que $y \in A \cup B$ e $y \in C$, de onde segue que $y \in (A \cup B) \cap C$. Desta forma, $(A \cap C) \cup (B \cap C) \subset (A \cup B) \cap C$.

Como as inclusões (1) e (2) são válidas, podemos concluir que a igualdade $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ é verdadeira para quaisquer conjuntos *A*, *B* e *C*. Assim, a propriedade apresentada é válida, o que conclui sua demonstração e, consequentemente, a tarefa proposta.

Desta forma, tendo concluído a demonstração em questão, você pode garantir que essa propriedade pode ser aplicada em qualquer situação e, desta forma, poderá explorar em sala de aula situações que envolvam o emprego desta na resolução de problemas práticos.

Faça valer a pena

1. Sejam os conjuntos dados por

$$A = \{-3, -2,\ 0,\ 2,\ 4,\ 6\}$$
$$B = \{-2,\ 2,\ 4,\ 5\}$$
$$C = \{-3,\ 2,\ 6\}$$

Em relação a esses conjuntos, foram apresentadas as seguintes afirmações:

I. O conjunto *C* está contido em *A* porque todo elemento de *C* pertence ao conjunto *A*.
II. O conjunto *B* pertence ao conjunto *A* porque todo elemento de *B* está contido em *A*.
III. O conjunto *C* pertence ao conjunto *A* porque todo elemento de *C* está contido em *A*.
IV. O conjunto *A* contém *B* porque todo elemento de *B* pertence ao conjunto *A*.

A respeito das afirmações apresentadas, assinale a alternativa correta:

a) Apenas a afirmação I está correta.
b) Apenas a afirmação IV está correta.
c) Apenas as afirmações I e II estão corretas.
d) Apenas as afirmações I e IV estão corretas.
e) Apenas as afirmações II e III estão corretas.

2. Os conjuntos podem ser descritos a partir da enumeração de seus elementos, segundo a descrição de uma propriedade ou na forma de diagramas, sendo essencial a compreensão dessas representações para a utilização do conceito de conjunto e de suas operações na interpretação de situações-problema.

Considere os conjuntos descritos no que segue:

$$M = \{x \mid x \text{ é um inteiro divisor de } 32\}$$
$$N = \{x \mid x \text{ é um inteiro tal que } 1 \leq x \leq 10\}.$$

Em relação aos conjuntos apresentados, assinale a alternativa que indica corretamente a união $M \cup N$ e a interseção $M \cap N$ relativa aos conjuntos *M* e *N*:

a) $M \cup N = \{1,2,4,8\}$ e $M \cap N = \{1,2,4,8\}$.
b) $M \cup N = \{1,2,3,4,5,6,7,8,9,10,16,32\}$ e $M \cap N = \varnothing$.
c) $M \cup N = \{1,2,3,4,5,6,7,8,9,10,16,32\}$ e $M \cap N = \{1,2,4,8\}$.
d) $M \cup N = \varnothing$ e $M \cap N = \{1,2,3,4,5,6,7,8,9,10,16,32\}$.
e) $M \cup N = \{1,2,3,4,5,6,7,8,9,10,12,16,32\}$ e $M \cap N = \{1,2,3,4,6,8\}$.

3. Visando organizar um campeonato escolar, a direção de uma instituição de ensino resolveu realizar uma pesquisa com seus alunos, identificando as modalidades esportivas preferidas dentre as seguintes possibilidades: futebol, voleibol e basquetebol.
Após a realização da pesquisa foi identificado que, dentre os 550 estudantes matriculados na instituição, 275 gostam de futebol, 227 de voleibol e 227 de basquetebol. Dentre esses estudantes, 95 gostam de futebol e voleibol, 82 gostam de voleibol e basquetebol, 52 gostam apenas de futebol e basquetebol, enquanto que 35 gostam dos três esportes. Também houveram 50 estudantes, dentre o total, que não opinaram nessa pesquisa.

Considerando as informações apresentadas, quantos estudantes preferem apenas futebol?

a) 52 estudantes.
b) 85 estudantes.
c) 93 estudantes.
d) 128 estudantes.
e) 275 estudantes.

Seção 1.2

Estudo das operações binárias

Diálogo aberto

Na primeira seção iniciamos os estudos de tópicos da Teoria de Conjuntos e Teoria de Números, analisando o que são conjuntos e elementos, identificando as relações de pertinência e inclusão, além de alguns conjuntos específicos e das operações união, interseção e diferença. Prosseguindo com os estudos, nessa seção o foco serão as operações binárias definidas sobre conjuntos, suas propriedades e as tábuas correspondentes, pois na definição de uma estrutura algébrica precisamos considerar, além de um conjunto, uma operação definida sobre este.

Desta forma, dando continuidade aos trabalhos enquanto chefe de equipe no escritório de consultoria, durante a resolução do problema anterior os funcionários recém-contratados pela empresa, e que passaram a integrar sua equipe, apresentaram dificuldades com as operações definidas a partir dos conjuntos numéricos, principalmente em relação à divisão e ao cálculo de porcentagem, o que demandou um tempo maior para a conclusão dos trabalhos.

Analisando os próximos problemas que precisam ser solucionados no atendimento à empresa de construção civil, você constatou a necessidade de propor um curso de capacitação a estes novos funcionários para que sua equipe seja mais eficiente no desenvolvimento das tarefas, pois a análise de dados exige conhecimentos a respeito dos conjuntos numéricos, das operações definidas sobre seus elementos e das propriedades que são satisfeitas.

Refletindo a respeito da importância dos conceitos indicados anteriormente para as ações executadas por sua equipe, você organizou o treinamento voltado ao estudo das operações binárias e suas principais propriedades.

Durante esse treinamento, os novos funcionários deverão executar as seguintes tarefas:

- Seja o conjunto $D = \{0,1,2,3\}$ e a operação Δ definida por: se $x, y \in D$ então $x \Delta y$ corresponde ao resto da divisão de $x + y$

por 4, considerando a operação usual de divisão no conjunto dos números naturais.

- Construa a tábua da operação Δ relativa ao conjunto D.
- Analise a tábua de operação e verifique se as propriedades associativa; comutativa; existência de elemento neutro; existência de elemento simétrico; e presença de elemento regular são satisfeitas.
- O conjunto D é uma parte fechada para a operação Δ? Como justificar esse fato?

Todas as questões que serão propostas ao longo da capacitação, conforme descrição anterior, têm por objetivo favorecer a compreensão dos conjuntos numéricos, suas operações e propriedades, por possibilitar a análise, de forma genérica, das propriedades que podem ser satisfeitas por diferentes operações definidas a partir de diversos conjuntos, visando capacitar os novos funcionários a trabalharem com estes conceitos em variadas situações. Nesse processo, a construção da tábua de operações poderá contribuir com a compreensão das propriedades que podem ser satisfeitas pelas operações binárias possibilitando, por meio da representação visual, a identificação das relações que podem ser estabelecidas entre os elementos do conjunto com base na operação correspondente.

Como os funcionários podem resolver estes problemas? Como você poderá orientá-los nestes estudos? Desenvolva a tarefa descrita e organize um roteiro de instruções para que você possa auxiliar os funcionários durante a realização das tarefas propostas no treinamento.

Não pode faltar

Operações binárias

Para dar início aos nossos estudos precisamos compreender o que é uma operação binária para que, na sequência, possamos estudar as propriedades correspondentes. É por meio da definição que podemos observar como os elementos do conjunto são combinados, a partir da operação em questão, para a geração de outros elementos do conjunto.

Para definir este conceito, considere um conjunto A não vazio. Uma **operação binária** (ou lei de composição interna) sobre o conjunto A corresponde a uma aplicação $f : A \times A \to A$, onde $A \times A$ refere-se ao produto cartesiano envolvendo o conjunto A.

Atenção

Uma aplicação $f : X \to Y$ corresponde a uma relação de X e Y na qual o domínio de f é o conjunto X e tal que a cada elemento $x \in X$ exista um único $y \in Y$ de modo que $f(x) = y$.

Sendo assim, uma operação binária é uma aplicação f que associa, a cada par ordenado $(x, y) \in A \times A$, um elemento $x * y$ (o qual pode ser lido como "x estrela y") pertencente ao conjunto A. O símbolo $*$ pode ser empregado para representar a operação definida a partir de f e, nesse caso, dizemos que A é um conjunto munido da operação $*$.

Assimile

Dependendo das características da operação $*$, podemos adotar outros símbolos para sua representação além de $*$, conforme indicado a seguir:

- Se $*$ é de característica aditiva, podemos empregar o símbolo $+$ e denominar a operação como adição. Neste caso, considera-se $x + y$ como soma e os elementos x e y são chamados de parcelas.
- Se $*$ tem caráter multiplicativo, adotamos o símbolo $\cdot$ e chamamos de multiplicação. Assim, o termo $x \cdot y$ ou xy é chamado de produto, enquanto que x e y são denominados fatores.

Podemos adotar também outros símbolos para a representação de operações genéricas, por exemplo: Δ, $\oplus$, $\otimes$ etc.

Exemplificando

Sendo $\mathbb{Z}$ o conjunto dos números inteiros, podemos definir a operação binária $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ dada por $f(x, y) = x + y$, a qual

corresponde à adição usual em $\mathbb{Z}$. Se $\mathbb{N}^* = \mathbb{N} - \{0\}$ a operação $f : \mathbb{N}^* \times \mathbb{N}^* \to \mathbb{N}^*$ com $f(x,y) = x^y$ é a potenciação definida sobre $\mathbb{N}^*$, a qual está bem definida, pois se $x, y \in \mathbb{N}^*$ então $x^y \in \mathbb{N}^*$.

Nem toda aplicação $f : A \times A \to A$, com A não vazio, será uma operação binária. Sejam $A = \mathbb{R}$ e $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ com $f(x,y) = x/y$, a qual corresponde à operação usual de divisão definida sobre $\mathbb{R}$. A aplicação *f* não define uma operação binária porque nem todo elemento de $\mathbb{R} \times \mathbb{R}$ está associado a algum elemento na imagem de *f*, como é o caso de $(1,0) \in \mathbb{R} \times \mathbb{R}$, pois $f(1,0)$ não está definido devido à impossibilidade de dividir 1 por 0 em $\mathbb{R}$. Logo, *f* não define uma aplicação e, por isso, não define uma operação binária. Porém, restringindo o domínio à $\mathbb{R}^* \times \mathbb{R}^*$, onde $\mathbb{R}^* = \mathbb{R} - \{0\}$, a aplicação $f : \mathbb{R}^* \times \mathbb{R}^* \to \mathbb{R}^*$ tal que $f(x,y) = x/y$ será uma operação binária ou lei de composição interna sobre R^*, correspondendo à divisão usual definida sobre $\mathbb{R}^*$.

Propriedades das operações binárias

Considere $*$ uma operação binária definida sobre um conjunto A não vazio. Vamos analisar algumas das propriedades que podem ser satisfeitas por $*$.

1) Propriedade associativa: a operação $*$ apresenta a propriedade **associativa** se, para todos $x, y, z \in A$, a igualdade $x * (y * z) = (x * y) * z$ for verificada. Por exemplo, as adições e multiplicações usuais nos conjuntos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ gozam da propriedade associativa, por isso são chamadas de "operações associativas". A adição definida sobre o conjunto $M_{m \times n}(\mathbb{R})$ das matrizes $m \times n$ com entradas reais é uma operação associativa. A potenciação sobre $\mathbb{N}^*$ não é associativa, pois $2 * (4 * 5) = 2 * (4^5) = 2^{(4^5)} = 2^{1024}$, $(2 * 4) * 5 = (2^4) * 5 = (2^4)^5 = 2^{20}$, e $2^{1024} \neq 2^{20}$. A divisão definida sobre $\mathbb{N}^*$ também não é associativa, identifique contraexemplos que justifiquem esse fato.

2) Propriedade comutativa: a operação $*$ apresenta a propriedade **comutativa** se, para todos $x, y \in A$, a igualdade $x * y = y * x$ for válida. Por exemplo, as operações usuais de adição e multiplicação definidas sobre os conjuntos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ apresentam a propriedade comutativa, sendo chamadas de "operações comutativas" nos conjuntos citados. A adição definida

sobre o conjunto $M_{m\times n}(\mathbb{R})$ é uma operação comutativa devido à validade da propriedade comutativa sobre as entradas das matrizes pertencentes a $M_{m\times n}(\mathbb{R})$, as quais são números reais. A divisão em $\mathbb{R}^*$ não é comutativa, pois para os números reais 4 e 8 temos $4/8 = 1/2 \neq 2 = 8/4$. A potenciação em $\mathbb{N}^*$ também não satisfaz a propriedade comutativa, pois, por exemplo, $3^2 = 9 \neq 8 = 2^3$.

3) Elemento neutro: a operação $*$ admite **elemento neutro** se existir $e \in A$ tal que $x * e = e * x = x$ para todo $x \in A$. É possível avaliar também os elementos neutros à esquerda ou à direita considerando, respectivamente, as expressões $e * x = x$ ou $x * e = x$. Note que a existência do elemento neutro $e \in A$ implica em e ser neutro à direita e à esquerda. Por exemplo, o zero corresponde ao elemento neutro para as operações usuais de adição definidas sobre $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$. Para as multiplicações usuais definidas sobre esses mesmos conjuntos, o elemento neutro é o 1. O elemento neutro da adição em $M_{m\times n}(\mathbb{R})$ é $0_{m\times n}$ (matriz nula do tipo $m \times n$), pois $0_{m\times n} + X = X + 0_{m\times n} = X$, qualquer que seja $X \in M_{m\times n}(\mathbb{R})$. A divisão em $\mathbb{R}^*$ admite 1 como elemento neutro à direita, pois $x/1 = x$ para todo $x \in \mathbb{R}^*$, mas não admite elemento neutro à esquerda, pois não existe um elemento $e \in \mathbb{R}^*$ fixo tal que $e/x = x$ para todo $x \in \mathbb{R}^*$, logo, o número 1 não é elemento neutro da divisão definida sobre $\mathbb{R}^*$.

4) Elementos simetrizáveis: se a operação $*$ admite elemento neutro $e \in A$, o elemento $x \in A$ é chamado de **elemento simetrizável** para a operação $*$ se existir $x' \in A$ de modo que $x * x' = x' * x = e$. Nesse caso, x' é chamado simétrico de x para a operação $*$. Veja que x ser simetrizável implica em x ser simetrizável à direita e à esquerda. Para uma operação aditiva, o elemento simétrico x' é chamado de oposto e denotado por $-x$, enquanto que na multiplicativa, x' é chamado de inverso e denotado por x^{-1}. Por exemplo, o 6 é um elemento simetrizável para a adição em $\mathbb{Z}$, com oposto -6, pois $6 + (-6) = (-6) + 6 = 0$. Esse número é também simetrizável em relação à multiplicação usual em $\mathbb{Q}$, com inverso $\frac{1}{6}$, pois $6 \cdot \frac{1}{6} = \frac{1}{6} \cdot 6 = 1$. Porém, 6 não é simetrizável para a multiplicação usual definida sobre $\mathbb{Z}$, pois não existe $x' \in \mathbb{Z}$ tal que $6 \cdot x' = x' \cdot 6$.

5) Elementos regulares: um elemento $a \in A$ é chamado de regular à esquerda em relação à $*$ quando, para quaisquer $x, y \in A$ com $a * x = a * y$, for verificado que $x = y$. De modo análogo, $a \in A$ é chamado de regular à direita em relação à $*$ quando ao considerar quaisquer $x, y \in A$ com $x * a = y * a$ for possível comprovar que $x = y$. Se $a \in A$ é regular à esquerda e à direita, então a é um **elemento regular** em relação à operação $*$ e, nesse caso, podemos dizer que a cumpre a lei do cancelamento em relação a $*$. Por exemplo, o 2 é regular em relação à adição e à multiplicação definidas em $\mathbb{Z}$, por satisfazer a lei do cancelamento para quaisquer $x, y \in \mathbb{Z}$. O zero não é regular em relação à multiplicação em $\mathbb{Z}$, pois $2 \cdot 0 = 3 \cdot 0$ e $2 \neq 3$. A matriz $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$ não é regular para a multiplicação em $M_2(\mathbb{R})$ pois $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 2 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 5 & -1 \\ 2 & 4 \end{pmatrix}$ e $\begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} \neq \begin{pmatrix} 5 & -1 \\ 2 & 4 \end{pmatrix}$.

6) Propriedade distributiva: dadas duas operações $*$ e $\oplus$ definidas sobre A, temos que $\oplus$ é distributiva à esquerda em relação à $*$ quando $x \oplus (y * z) = (x \oplus y) * (x \oplus z)$ para todos $x, y, z \in A$. Analogamente, $\oplus$ é **distributiva** à direita em relação à $*$ quando tivermos $(y * z) \oplus x = (y \oplus x) * (z \oplus x)$ para quaisquer $x, y, z \in A$. Quando $\oplus$ for distributiva à esquerda e à direita em relação à $*$, $\oplus$ será distributiva em relação à $\oplus$. Por exemplo, a multiplicação é distributiva em relação à adição, ambas definidas sobre $\mathbb{Z}$. A multiplicação definida sobre $M_n(\mathbb{R})$ é distributiva em relação à adição definida sobre esse mesmo conjunto, pois, para quaisquer $X, Y, Z \in M_2(\mathbb{R})$, são válidas as expressões $X \cdot (Y + Z) = (X \cdot Y) + (X \cdot Z)$ e $(Y + Z) \cdot X = (Y \cdot X) + (Z \cdot X)$. A potenciação sobre $\mathbb{N}^*$ não é distributiva em relação à multiplicação, pois em $\mathbb{N}^*$ é válido que $(x \cdot y)^z = x^z \cdot y^z$, com $x, y, z \in \mathbb{N}^*$, sendo a potenciação distributiva à direita em relação à multiplicação, o que não ocorre à esquerda, porque $4^{2 \cdot 3} = 4096 \neq 1024 = 4^2 \cdot 4^3$.

Faça você mesmo

Prove que no caso da operação $*$ definida sobre A admitir um elemento neutro $e \in A$, então este elemento é único em A.

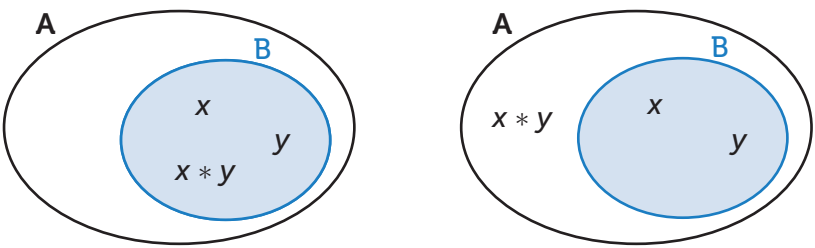
Reflita

As propriedades das operações binárias podem ser empregadas na resolução dos mais variados problemas, como as equações polinomiais por exemplo. Que propriedades das operações de adição e multiplicação usuais, definidas sobre o conjunto de números reais, devem ser empregadas quando desejamos resolver uma equação do 1º grau na forma $ax + b = c$?

Parte fechada para uma operação

Considere $*$ uma operação definida sobre um conjunto A e seja $B \subset A$ um subconjunto não vazio de A. O conjunto B é classificado como uma **parte fechada** de A para a operação $*$ se, e somente se, para quaisquer $x, y \in B$ for verificado que $x * y \in B$. Na Figura 1.9(a) é apresentado um diagrama que ilustra o conjunto B como parte fechada de A para a operação $*$, enquanto que a Figura 1.9(b) ilustra um caso em que B não é parte fechada de A para $*$.

Figura 1.9 | Parte fechada para operações



(*a*) Parte fechada para $*$ (*b*) Parte não fechada para $*$

Fonte: elaborada pelo autor.

Exemplificando

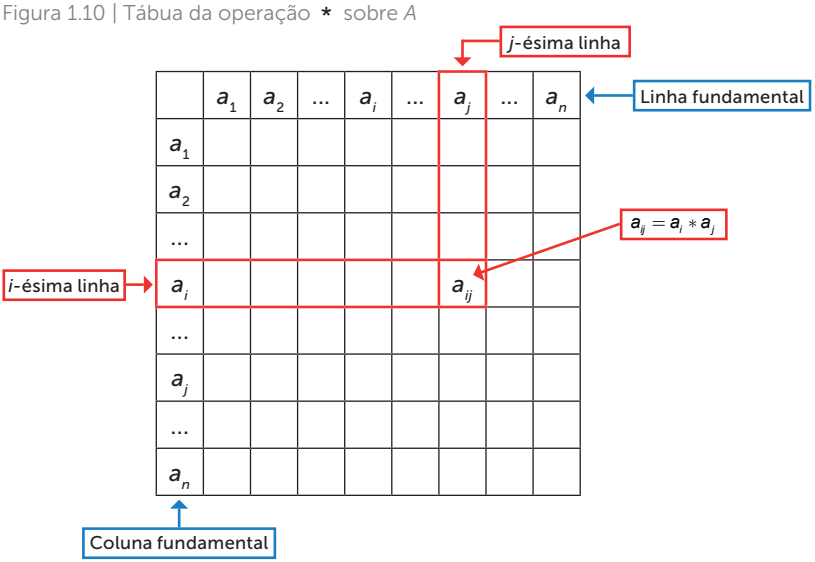
$\mathbb{Q}$ é uma parte fechada para as operações de adição e multiplicação usuais definidas em $\mathbb{R}$. Note que $\mathbb{Q} \neq \varnothing$, $\mathbb{Q} \subset \mathbb{R}$ e para quaisquer $x, y \in \mathbb{Q}$ temos que $x + y,\ xy \in \mathbb{Q}$. O conjunto $\mathbb{R} - \mathbb{Q}$ dos números irracionais não é parte fechada para a adição e multiplicação em $\mathbb{R}$, pois $\sqrt{3}, -\sqrt{3} \in \mathbb{R} - \mathbb{Q}$, $\sqrt{3} + \left(-\sqrt{3}\right) = 0 \notin \mathbb{R} - \mathbb{Q}$ e $\left(\sqrt{3}\right)\left(-\sqrt{3}\right) = -3 \notin \mathbb{R} - \mathbb{Q}$.

Tábua de operação

Quando uma operação é definida sobre um conjunto contendo uma quantidade finita de elementos, podemos representá-la a partir de uma tábua de operação.

Seja $A = \{a_1, a_2, ..., a_n\}$, com $n > 1$. Considere a operação $f : A \times A \to A$ representada por $*$ e que associa a cada par (a_i, a_j) o elemento $a_i * a_j = a_{ij}$, para $1 \leq i \leq n$ e $1 \leq j \leq n$. A partir dessas informações, a tábua da operação $*$ é construída indicando, na linha fundamental e na coluna fundamental, os elementos de A, e adotando as interseções entre linhas e colunas paralelas às fundamentais como os elementos resultantes da aplicação da operação $*$ sobre os elementos correspondentes. A estrutura da tábua da operação $*$ sobre A é descrita conforme a Figura 1.10.

Figura 1.10 | Tábua da operação $*$ sobre A



Fonte: elaborada pelo autor.

Exemplificando

Considere o conjunto $X = \{-1, 0, 1\}$ e a operação de multiplicação definida sobre $\mathbb{Z}$ e restrita a X. Note que $(-1)\cdot(-1) = 1$, $(-1)\cdot 0 = 0$, $(-1)\cdot 1 = -1$, $0\cdot(-1) = 0$, $0\cdot 0 = 0$, $0\cdot 1 = 0$, $1\cdot(-1) = -1$, $1\cdot 0 = 0$ e $1\cdot 1 = 1$. A tábua da operação de multiplicação sobre X é descrita conforme a Figura 1.11.

Figura 1.11 | Tábua da operação de multiplicação sobre o conjunto *X*

.	–1	0	1
–1	1	0	–1
0	0	0	0
1	–1	0	1

Fonte: elaborada pelo autor.

Na construção da tábua de uma operação evidenciamos todas as combinações possíveis entre os elementos do conjunto em relação à operação definida. Podemos também observar as propriedades satisfeitas pela operação a partir de sua tábua.

No estudo das propriedades associadas à tábua de operação, considere um conjunto $A=\{a_1,a_2,...,a_n\}$, com $n>1$, e uma operação binária $*$ definida sobre A. A estrutura da tábua da operação $*$ é ilustrada de acordo com a Figura 1.10. Em relação a essa operação temos:

1) Propriedade associativa: é necessário avaliar os elementos disponíveis na tábua e efetuar os produtos na forma $a_i * a_{jk}$ e $a_{ij} * a_k$, para todos $i,j,k \in \{1,2,...,n\}$, comparando-os; caso esses produtos sejam iguais, conclui-se que a operação $*$ é associativa. Para um conjunto $A=\{x,y,z\}$, na Figura 1.12(a) temos um exemplo de operação associativa $*$ definida sobre A e na Figura 1.12(b), uma operação não associativa sobre A, pois $z*(x*y)=z$ e $(z*x)*y=y$, por exemplo.

Figura 1.12 | Tábuas de operações associativas e não associativas

*	x	y	x
x	x	y	x
y	z	y	x
z	z	y	z

(a) Propriedade associativa

*	x	y	z
x	x	z	x
y	x	y	x
z	z	y	z

(b) Propriedade não associativa

Fonte: elaborada pelo autor.

2) Propriedade comutativa: temos a diagonal principal da tábua composta pelos elementos $a_{11}, a_{22}, \ldots, a_{nn}$; note que a_{ij} e a_{ji} ocupam posições simétricas em relação à diagonal principal; assim, $*$ será comutativa se a tábua correspondente for simétrica em relação à diagonal principal. Para um conjunto $A = \{x, y, z\}$, na Figura 1.13(a) temos um exemplo de operação comutativa definida sobre A e na Figura 1.13(b), uma operação não comutativa sobre A, pois $z * x \neq x * z$ e $z * y \neq y * z$.

Figura 1.13 | Tábuas de operações comutativas e não comutativas

$*$	x	y	z
x	z	x	y
y	x	y	z
z	y	z	x

(a) Propriedade comutativa

$*$	x	y	z
x	z	x	y
y	x	y	z
z	z	y	x

(b) Propriedade não comutativa

Fonte: elaborada pelo autor.

3) Existência de elemento neutro: da tábua da operação $*$, se for possível identificar um elemento $e \in A$ tal que a coluna a que o mesmo pertença seja igual à coluna fundamental, e que a linha correspondente a e seja igual à linha fundamental, podemos concluir que e é o elemento neutro da operação $*$. A partir do conjunto $A = \{x, y, z\}$, na Figura 1.14(a) podemos observar a definição da operação $*$ que possui y como elemento neutro, enquanto na operação ilustrada na Figura 1.14(b) não há a presença de elemento neutro, pois não existem linhas ou colunas da tábua iguais às fundamentais.

Figura 1.14 | Tábuas de operações e a presença de elemento neutro

$*$	x	y	z
x	z	x	y
y	x	y	z
z	y	z	x

(a) Elemento neutro y

$*$	x	y	z
x	z	x	y
y	x	z	y
z	z	y	x

(b) Ausência de elemento neutro

Fonte: elaborada pelo autor.

4) Existência de elemento simetrizável: para um elemento $a \in A$, se for possível identificar a presença de e (elemento neutro) ao menos uma vez na linha e na coluna a que a pertence, de modo que as posições ocupadas por e na linha e coluna consideradas sejam simétricas em relação à diagonal principal, podemos dizer que a é simetrizável. Na Figura 1.15(a) temos uma operação com elemento neutro (y) e elemento simetrizável ($x \in A$, por exemplo), enquanto que na Figura 1.15(b) não há presença destes tipos de elementos.

Figura 1.15 | Tábuas de operações e a presença de elementos simetrizáveis e regulares

*	x	y	z
x	z	x	y
y	x	y	z
z	y	z	x

(a) Presença de elemento simetrizável e regular

*	x	y	z
x	z	x	y
y	x	y	y
z	z	z	x

(b) Ausência de elemento simetrizável e regular

Fonte: elaborada pelo autor.

5) Existência de elemento regular: para que um elemento $a \in A$ seja regular, é necessário e suficiente que na linha e na coluna da tábua da operação $*$ a que a pertença não existam elementos repetidos. Na Figura 1.15(a) temos a presença de elemento regular, $x \in A$, por exemplo, enquanto que na Figura 1.15(b) não existem elementos regulares, pois na linha e coluna relativas a z, e na coluna relativa a x, existe a repetição de termos.

Assimile

Podemos construir a tábua de uma operação $*$, definida sobre um conjunto não vazio A finito, indicando todos os elementos do conjunto na linha e coluna fundamentais e indicando os resultados a partir das interseções entre linhas e colunas paralelas às fundamentais. Por meio desta, é possível visualizar todas as combinações possíveis dos elementos de A por $*$ e verificar as propriedades satisfeitas pela operação $*$ a partir da estrutura citada.

Pesquise mais

Consulte o primeiro tópico chamado "Aplicações binárias" do material "Ensino Superior: Álgebra: Grupos", o qual apresenta um resumo a respeito das operações/aplicações binárias e suas propriedades. Disponível em: <http://www.uel.br/projetos/matessencial/superior/algebra/grupos.htm>. Acesso em: 16 abr. 2018.

Sem medo de errar

No contexto de atuação como funcionário do escritório de consultoria, você precisa organizar as tarefas a serem desenvolvidas em um curso de capacitação a ser aplicado aos funcionários de sua equipe. Neste treinamento, as tarefas serão desenvolvidas com base no conjunto $D = \{0,1,2,3\}$ e na operação Δ dada por: se $x, y \in D$ então $x \Delta y$ corresponde ao resto da divisão de $x + y$ por 4, considerando a operação usual de divisão no conjunto dos números naturais.

A primeira tarefa a ser executada pelos funcionários consiste na construção da tábua da operação Δ relativa ao conjunto D. Uma das aplicações importantes desta estrutura é a possibilidade da visualização rápida dos resultados obtidos a partir da aplicação de Δ sobre os elementos de D, por meio das interseções entre linhas e colunas paralelas às fundamentais, o que pode agilizar a resolução dos problemas em estudo. Para a construção da tábua é necessário avaliar todas as combinações possíveis entre elementos de D a partir de Δ. Alguns exemplos são:

- $0 + 0 = 0$ e o resto da divisão de 0 por 4 é igual a 0, logo $0 \Delta 0 = 0$;
- $0 + 1 = 1$ e o resto da divisão de 1 por 4 é igual a 1, logo $0 \Delta 1 = 1$;
- $1 + 2 = 3$ e o resto da divisão de 3 por 4 é igual a 3, logo $1 \Delta 2 = 3$;
- $1 + 3 = 4$ e o resto da divisão de 4 por 4 é igual a 0, logo $1 \Delta 3 = 0$.

Tomando as demais combinações, sabendo que as únicas possibilidades de restos da divisão de números naturais por 4 são 0, 1, 2 ou 3, a tábua da operação Δ é dada na Figura 1.16.

Figura 1.16 | Tábua da operação Δ definida sobre *D*

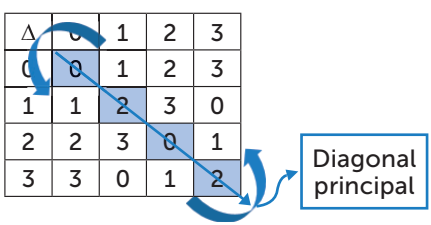
Δ	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Fonte: elaborada pelo autor.

Pela tábua apresentada na Figura 1.16, temos que a operação Δ é associativa, o que pode ser justificado a partir da avaliação da igualdade $x\Delta(y\Delta z)=(x\Delta y)\Delta z$ para todos $x,y,z\in D$. Note, por exemplo, que $0\Delta(1\Delta 2)=3=(0\Delta 1)\Delta 2$, $0\Delta(2\Delta 1)=3=(0\Delta 2)\Delta 1$, $0\Delta(1\Delta 1)=2=(0\Delta 1)\Delta 1$ etc. Para concluir essa justificativa, construa as demais combinações entre elementos de D, investigando a validade da igualdade destacada para todos os elementos de D.

A operação Δ é comutativa, pois a tábua é simétrica em relação à sua diagonal principal, o que pode ser analisado com base na Figura 1.17(a). Além disso, existe elemento neutro Δ, que corresponde ao $0\in D$, porque a linha e a coluna relativas a esse número coincidem com a linha fundamental e com a coluna fundamental, respectivamente, como destacado na Figura 1.17(b).

Figura 1.17 | Análise da tábua da operação Δ definida sobre *D*



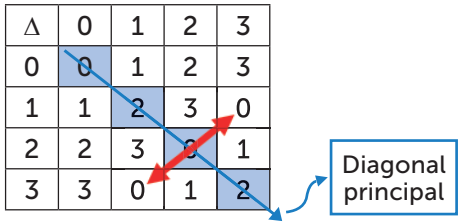
Δ	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

(a) Propriedade comutativa **(b) Existência de elemento neutro**

Fonte: elaborada pelo autor.

Note que os números 1 e 3 são simetrizáveis para a operação Δ porque nas linhas e colunas associadas a esses elementos existe a presença do zero e, para estes números, os elementos neutros são simétricos em relação à diagonal principal, o que é evidenciado na Figura 1.18.

Figura 1.18 | Elementos simetrizáveis associados a Δ



Fonte: elabora pelo autor.

Também da Figura 1.18 observamos que o número 2 é simetrizável, pois como o zero está presente na linha e coluna correspondentes a esse elemento e o zero pertence à diagonal principal, o elemento neutro satisfaz a propriedade da simetria. O elemento neutro 0 é também simetrizável, já que zero pertence à diagonal principal da tábua, satisfazendo à condição de simetria. Logo, todos os elementos de D são simetrizáveis em relação à operação Δ.

Veja que todas as linhas e colunas da tábua da operação Δ possuem algum dos elementos igual a zero e, além disso, todos os elementos que pertencem a uma mesma linha ou coluna são distintos. Logo, todos os elementos de D são regulares em relação a Δ.

Em síntese, a operação Δ é associativa, comutativa, apresenta elemento neutro, elementos simetrizáveis e regulares. Também o conjunto D é uma parte fechada para a operação Δ, porque na tábua da operação Δ podemos constatar que $x\Delta y \in D$, desde que $x, y \in D$, porque as únicas possibilidades de resto da divisão de um número natural por 4 são 0, 1, 2 ou 3, isto é, os elementos que compõem o conjunto D. Portanto, D pode ser classificado como parte fechada de $\mathbb{N}$ para a operação Δ.

Com essas propriedades sendo satisfeitas, os funcionários podem empregá-las na resolução de outros problemas que tomem por base esse conjunto e a operação estudada, garantindo que sempre podemos combinar elementos do conjunto D pela operação Δ, gerando elementos de D, por se tratar de uma parte fechada. Além disso, ao consultar a tábua, os funcionários conseguirão obter mais rapidamente os resultados por meio da avaliação das interseções entre linhas e colunas.

Assim, para a conclusão dessa tarefa, basta organizar todas as informações em um roteiro de modo a organizar a capacitação a ser desenvolvida com os funcionários, indicando, para cada parte do curso, os principais conceitos a serem explorados.

Avançando na prática

Tábuas de operações relacionadas às famílias de conjuntos

Descrição da situação-problema

Os conjuntos numéricos, conforme abordados na Educação Básica, satisfazem à relação de inclusão $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$. A partir destes conjuntos, considere a família $F = \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$ composta por esses conjuntos e suponha que, sobre F, seja definida a operação de interseção entre conjuntos, conforme caracterização apresentada na seção anterior, e representada por $\cap$.

Suponha que você precisa organizar uma aula para a Educação Básica comparando os diferentes conjuntos numéricos a partir das inclusões observadas. Para isso, podemos construir afirmações como as seguintes, de modo a evidenciar as relações entre esses conjuntos:

- Todo número natural é um número real;
- Todo número inteiro é um número racional.

Com base nesse contexto, construa a tábua correspondente a operação de interseção definida sobre *F*, conforme descrição anterior, e identifique o elemento neutro associado à operação de interseção entre conjuntos definida sobre *F*. Qual é o significado desse elemento neutro no contexto apresentado, envolvendo os conjuntos numéricos?

Resolução da situação-problema

Temos que se A e B são conjuntos tais que $B \subset A$ então $A \cap B = B$. Sendo assim, da relação $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ temos, por exemplo, que: $\mathbb{N} \cap \mathbb{Z} = \mathbb{N} = \mathbb{Z} \cap \mathbb{N}$; $\mathbb{Z} \cap \mathbb{Q} = \mathbb{Z} = \mathbb{Q} \cap \mathbb{Z}$; $\mathbb{R} \cap \mathbb{Q} = \mathbb{Q} = \mathbb{Q} \cap \mathbb{R}$; $\mathbb{N} \cap \mathbb{Q} = \mathbb{N} = \mathbb{Q} \cap \mathbb{N}$ etc.

Além disso, a operação de interseção entre conjuntos é tal que $A \cap A = A$ para todo conjunto A. Logo, no caso do problema em estudo, por exemplo, $\mathbb{Q} \cap \mathbb{Q} = \mathbb{Q}$.

Considerando as informações apresentadas, temos que a tábua da operação de interseção pode ser dada conforme a Figura 1.19.

Figura 1.19 | Tábua da operação de interseção de conjuntos definida sobre *F*

$\cap$	$\mathbb{R}$	$\mathbb{Q}$	$\mathbb{Z}$	$\mathbb{N}$
$\mathbb{R}$	$\mathbb{R}$	$\mathbb{Q}$	$\mathbb{Z}$	$\mathbb{N}$
$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Z}$	$\mathbb{N}$
$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{N}$
$\mathbb{N}$	$\mathbb{N}$	$\mathbb{N}$	$\mathbb{N}$	$\mathbb{N}$

Fonte: elaborado pelo autor.

Observe que a linha que contém o conjunto $\mathbb{R}$ é igual à linha fundamental. Além disso, a coluna referente a $\mathbb{R}$ é igual à coluna fundamental. Assim, $\mathbb{R}$ corresponde ao elemento neutro da operação de interseção entre conjuntos definida a partir da família *F*. Portanto, $\mathbb{R}$ corresponde ao conjunto que, ao ser comparado com qualquer um dos outros conjuntos de *F* pela interseção, sempre retornará como resultado o outro conjunto envolvido, o que reforça o fato de todos os demais conjuntos estarem contidos em $\mathbb{R}$ e que, no contexto apresentado, o elemento neutro corresponde àquele conjunto que contém todos os demais, possibilitando a construção das seguintes afirmações: todo número natural é real, todo número inteiro é real e todo número racional é real.

Faça valer a pena

1. Considere o conjunto de números reais $\mathbb{R}$. Com base nesse conjunto, construiu-se a operação binária $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ dada por $x * y = \frac{x+y}{2}$ para todos $x, y \in \mathbb{R}$.
Em relação à operação apresentada, foram apresentadas as seguintes afirmações e uma relação proposta entre elas:

I. A operação $*$ sobre $\mathbb{R}$ satisfaz a propriedade associativa.
PORQUE
II. A operação $*$ sobre $\mathbb{R}$ é comutativa.

Em relação às afirmações apresentadas, assinale a alternativa correta:

a) As afirmações I e II estão corretas, e a II é uma justificativa correta para a I.
b) As afirmações I e II estão corretas, mas a II não é uma justificativa correta para a I.
c) A afirmação I está correta, enquanto que a II está incorreta.
d) A afirmação I está incorreta, enquanto que a II está correta.
e) As afirmações I e II estão incorretas.

2. Considere o conjunto dos números inteiros $\mathbb{Z}$ e a operação de multiplicação usual definida sobre esse conjunto. Além disso, sejam os subconjuntos de $\mathbb{Z}$ descritos a seguir:

$$A = \{x \in \mathbb{Z} \mid x < 0\}$$
$$B = \{x \in \mathbb{Z} \mid x \text{ é par}\}$$
$$C = \{x \in \mathbb{Z} \mid x \text{ é ímpar}\}$$
$$D = \{x \in \mathbb{Z} \mid x \text{ é primo}\}.$$

Com base nas informações apresentadas, assinale a alternativa que indica quais dos subconjuntos descritos podem ser classificados como partes fechadas de $\mathbb{Z}$ para a operação de multiplicação usual:

a) Apenas os subconjuntos A e B.
b) Apenas os subconjuntos A e C.
c) Apenas os subconjuntos B e C.
d) Apenas os subconjuntos B e D.
e) Apenas os subconjuntos C e D.

3. Com base no conjunto $E = \{1, 2, 3, 4\}$, foi construída a operação Δ cuja tábua de operação é dada como segue:

Em relação à operação Δ definida sobre E, analise as seguintes afirmações, classificando-as como verdadeiras (V) ou falsas (F):

( ) O elemento $(3\Delta 2)\Delta 4$ é igual ao elemento $4\Delta 3$.
( ) O elemento $\left[4\Delta(3\Delta 1)\right]\Delta 4$ é igual ao elemento $3\Delta 3$.
( ) A operação Δ satisfaz a propriedade comutativa.
( ) O elemento neutro de Δ corresponde ao número 4.

Assinale a alternativa que indica a sequência correta, considerando a ordem na qual as afirmações foram apresentadas:

a) V – F – F – V.
b) V – F – V – F.
c) V – V – F – F.
d) F – V – F – V.
e) F – F – V – V.

Seção 1.3

Estruturas Algébricas: Conjuntos Numéricos

Diálogo aberto

Na seção anterior investigamos as operações binárias e suas propriedades, observando como podemos construir e analisar uma tábua associada a uma operação. Ainda relacionado a esse tema, nessa terceira seção estudaremos as características dos conjuntos numéricos com suas operações e propriedades, bem como as caracterizações do mínimo múltiplo comum e do máximo divisor comum. Esses conteúdos são abordados desde a Educação Básica e são essenciais para que os alunos possam interpretar as mais variadas situações do cotidiano nas quais os números são empregados, ou seja, as diversas funções sociais assumidas pelo número, como nas identificações em documentos, números de telefones, códigos postais, entre outros, sendo necessário, para isso, o conhecimento dos principais conjuntos numéricos.

Considerando esses objetivos, após a realização do treinamento descrito na seção anterior, você e sua equipe precisam finalizar o atendimento à empresa de construção civil. A última situação a ser resolvida por vocês consiste na organização das numerações de residências em um empreendimento que será lançado em breve pela empresa em questão.

A empresa da área de construção civil construiu um condomínio horizontal composto por diversas residências e precisa organizar as numerações das casas localizadas em cada rua. Ao invés de adotar os procedimentos usuais, como o cálculo das distâncias das casas até um ponto fixo, que em geral corresponde ao ponto inicial das ruas, decidiu-se adotar uma nova estratégia para a determinação das numerações das residências devido a um padrão adotado pela empresa de distribuição uniforme destas em cada rua do empreendimento. Com esse procedimento, a empresa pretende evitar muitas repetições nas numerações das casas, contribuindo assim para agilizar a localização destas pelos moradores e visitantes. No procedimento desejado pela empresa, na primeira rua do condomínio, as seis casas serão numeradas da seguinte forma:

$\frac{z}{6}, \frac{z}{5}, \frac{z}{4}, \frac{z}{3}, \frac{z}{2}, z$ e nesta ordem, sabendo que z é um número inteiro e, além disso, z é o menor número positivo para o qual todos os números apresentados são inteiros. Em resumo, z deve ser o menor número inteiro para o qual $\frac{z}{6}, \frac{z}{5}, \frac{z}{4}, \frac{z}{3}, \frac{z}{2}$ e z sejam todos números inteiros.

Refletindo sobre a situação desta primeira rua, qual será a numeração de cada casa? Que procedimentos devem ser empregados para a identificação de z e dos números em questão?

Resolva este problema propondo um roteiro de instruções para a determinação das numerações das casas, pois um procedimento análogo será usado pelos funcionários da empresa na identificação das numerações das casas das demais ruas do condomínio horizontal.

Com a resolução deste problema, você e sua equipe já possuirão todas as informações solicitadas pela empresa ao escritório de consultoria. Desta forma, para concluir os trabalhos, você deverá organizar o relatório final, apresentando as informações solicitadas para serem encaminhadas à empresa atendida.

Não pode faltar

O trabalho com os conjuntos numéricos é iniciado na Educação Infantil pelos números naturais em associação com a contagem. Nas etapas seguintes, os demais conjuntos são introduzidos considerando suas operações usuais e propriedades. Devido a esse fato, o conhecimento desses conjuntos é essencial ao professor para que este possa organizar suas aulas de modo a favorecer a aprendizagem destes temas pelos alunos. Além disso, esses conceitos serão essenciais para, por exemplo, o trabalho com as funções, as sequências, para a resolução de problemas que envolvam os conjuntos numéricos, entre outros. Assim, nessa seção, iniciaremos nossos estudos por esse tema.

Conjuntos numéricos

O **conjunto dos números naturais** teve seu desenvolvimento associado à necessidade do homem em realizar a contagem visando a quantificação de seus bens. Partindo do número zero,

o conjunto dos números naturais pode ser apresentado como: $\mathbb{N} = \{0, 1, 2, 3, 4, ...\}$. Se excluirmos o zero desse conjunto, teremos o conjunto dos naturais não nulos, descrito por: $\mathbb{N}^* = \{1, 2, 3, 4, ...\}$.

Historicamente, o matemático Giuseppe Peano (1858-1932) foi o responsável pela proposição dos chamados **axiomas de Peano**, afirmações aceitas sem demonstração e que visam a estruturação do conjunto de números naturais (BOYER, 1974, p.436). Para isso, esse matemático selecionou os conceitos primitivos "zero", "número" (inteiro não negativo) e "sucessor", a partir dos quais construiu as seguintes afirmações:

1. O zero é um número.
2. Se a é um número, então o sucessor de a é também um número.
3. O zero não é o sucessor de algum número, ou seja, zero é o único número que não é sucessor de outro número.
4. Números diferentes estão associados a sucessores distintos.
5. Se um conjunto S de números contém o zero e o sucessor de todo número de S, então todo número está em S, ou seja, S contém todos os números (afirmação conhecida como axioma da indução).

A partir do conjunto de números naturais, podemos definir duas operações binárias: a adição $(+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N})$ e a multiplicação $(\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N})$ usuais, respectivamente, como $x + y$ e $x \cdot y = xy$ para todos $x, y \in \mathbb{N}$, as quais gozam das propriedades indicadas na Tabela 1.1.

Tabela 1.1 | Propriedades das operações usuais definidas sobre $\mathbb{N}$

Propriedades	Adição usual $(+)$	Multiplicação usual $(\cdot)$
Associativa	Para todos $x, y, z \in \mathbb{N}$ tem-se $(x + y) + z = x + (y + z)$.	Para todos $x, y, z \in \mathbb{N}$ tem-se $(xy)z = x(yz)$.
Comutativa	Para todos $x, y \in \mathbb{N}$ tem-se $x + y = y + x$.	Para todos $x, y \in \mathbb{N}$ tem-se $xy = yx$.

Existência de elemento neutro	Existe $0 \in \mathbb{N}$ tal que, para todo $x \in \mathbb{N}$, tem-se $0 + x = x + 0 = x$.	Existe $1 \in \mathbb{N}$ tal que, para todo $x \in \mathbb{N}$, tem-se $1 \cdot x = x \cdot 1 = x$.
Distributiva	Se $x, y, z \in \mathbb{N}$ tem-se $x(y + z) = xy + xz$ e $(y + z)x = yx + zx$.	

Fonte: elaborada pelo autor.

Exemplificando

Podemos ainda definir a operação usual de subtração $- : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ dada por $x - y$ para $x, y \in \mathbb{N}$, a qual não é comutativa, pois, por exemplo, $3 - 2 = 1$ e $2 - 3 \notin \mathbb{N}$; não é associativa, pois temos que $4 - (3 - 1) = 2$, $(4 - 3) - 1 = 0$ e $2 \neq 0$, por exemplo; e não admite elemento neutro, pois não existe $a \in \mathbb{N}$ tal que $a - x = x - a$ para todo $x \in \mathbb{N}$.

Reflita

Como são estruturados os algoritmos das operações de adição, subtração e multiplicação definidas sobre $\mathbb{N}$, abordados na Educação Básica?

Um outro conjunto abordado na Educação Básica é o dos números inteiros, dado por $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$, o qual inclui os números naturais e os inteiros negativos.

Podemos ainda analisar os seguintes subconjuntos de $\mathbb{Z}$:

- Subconjunto dos inteiros não negativos: $\mathbb{Z}_+ = \{0, 1, 2, 3, ...\}$;
- Subconjunto dos inteiros não positivos: $\mathbb{Z}_- = \{0, -1, -2, -3, ...\}$;
- Subconjunto dos inteiros não nulos: $\mathbb{Z}^* = \{..., -3, -2, -1, 1, 2, 3, ...\}$;
- Subconjunto dos inteiros positivos: $\mathbb{Z}_+^* = \{1, 2, 3, 4, ...\}$;
- Subconjunto dos inteiros negativos: $\mathbb{Z}_-^* = \{-1, -2, -3, -4, ...\}$.

As operações de adição e multiplicação usuais definidas sobre o conjunto dos números inteiros gozam das propriedades indicadas na Tabela 1.2.

Tabela 1.2 | Propriedades das operações usuais definidas sobre $\mathbb{Z}$

Propriedades	Adição usual $(+)$	Multiplicação usual $(\cdot)$
Associativa	Para todos $x, y, z \in \mathbb{Z}$ tem-se $(x+y)+z=x+(y+z)$.	Para todos $x, y, z \in \mathbb{Z}$ tem-se $(xy)z=x(yz)$.
Comutativa	Para todos $x, y \in \mathbb{Z}$ tem-se $x+y=y+x$.	Para todos $x, y \in \mathbb{Z}$ tem-se $xy=yx$.
Existência de elemento neutro	Existe $0 \in \mathbb{Z}$ tal que, para todo $x \in \mathbb{Z}$, tem-se $0+x=x+0=x$.	Existe $1 \in \mathbb{Z}$ tal que, para todo $x \in \mathbb{Z}$, tem-se $1 \cdot x=x \cdot 1=x$.
Existência de elemento simétrico	Para todo $x \in \mathbb{Z}$, existe $-x \in \mathbb{Z}$ tal que $(-x)+x=x+(-x)=0$.	A existência de elemento simétrico não é satisfeita para a multiplicação
Distributiva	Se $x, y, z \in \mathbb{Z}$ tem-se $x(y+z)=xy+xz$ e $(y+z)x=yx+zx$	

Fonte: elaborada pelo autor.

Faça você mesmo

Defina a operação usual de subtração sobre o conjunto de números inteiros e identifique as propriedades que são satisfeitas em relação a essa operação.

O **conjunto dos números racionais** é composto pelos números na forma $\frac{p}{q}$, em que $p, q \in \mathbb{Z}$ e $q \neq 0$, ou ainda, descrito por: $\mathbb{Q}=\left\{\frac{p}{q}; p \in \mathbb{Z} \text{ e } q \in \mathbb{Z}^*\right\}$. Esse conjunto inclui os números naturais, inteiros, as frações positivas e negativas.

Em relação às operações usuais de adição e multiplicação definidas sobre $\mathbb{Q}$, as seguintes propriedades são satisfeitas: associatividade, comutatividade, existência de elemento neutro, existência de elemento simétrico (na multiplicação para todo racional não nulo) e distributividade.

Reflita

Como podemos justificar que a soma de dois números racionais é sempre um número racional?

O **conjunto dos números reais** $\mathbb{R}$ é composto pelos números racionais, pertencentes ao conjunto $\mathbb{Q}$ conforme descrição anterior, e os irracionais, como é o caso dos números π e $\sqrt{2}$, por exemplo, os quais pertencem a $\mathbb{R}-\mathbb{Q}$ e correspondem às dízimas não periódicas. Assim, temos $\mathbb{R}=\mathbb{Q}\cup\left(\mathbb{R}-\mathbb{Q}\right)$.

Assim como em $\mathbb{Q}$, as operações usuais de adição e multiplicação definidas sobre $\mathbb{R}$ gozam das seguintes propriedades: associatividade; comutatividade; existência de elemento neutro; existência de elemento simétrico (na multiplicação para todo real não nulo); e distributividade.

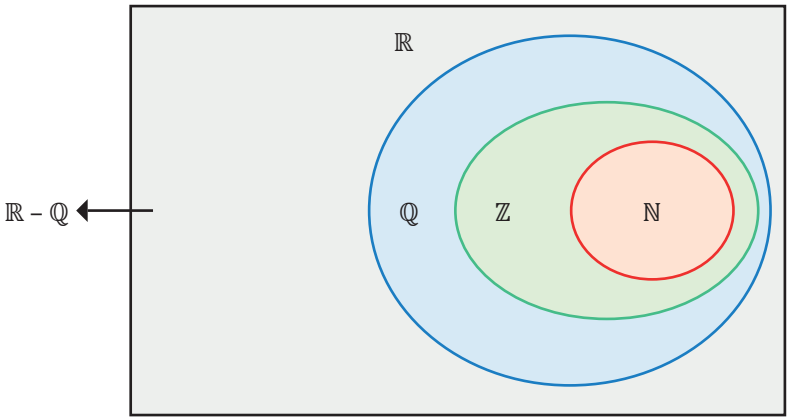
Relações entre os conjuntos numéricos

Os conjuntos numéricos descritos anteriormente podem ser relacionados entre si a partir da relação de inclusão de conjuntos. Note que:

- Todo número natural é inteiro, então $\mathbb{N}\subset\mathbb{Z}$;
- Todo número inteiro é também racional, logo, $\mathbb{Z}\subset\mathbb{Q}$;
- Qualquer número racional é também real, de onde segue que $\mathbb{Q}\subset\mathbb{R}$;
- O conjunto de números reais pode ser dado por $\mathbb{R}=\mathbb{Q}\cup\left(\mathbb{R}-\mathbb{Q}\right)$.

As relações destacadas podem ser observadas no diagrama da Figura 1.20.

Figura 1.20 | Relações de inclusão entre os conjuntos numéricos



Fonte: elaborada pelo autor.

A partir da Figura 1.20 podemos visualizar as relações de inclusão e, consequentemente, as relações de pertinência envolvendo números e conjuntos numéricos.

Pesquise mais

Acesse a Seção 1.1.1 do livro "Estruturas Algébricas", de Julio C. Cochmanski e Liliane C. de C. Cochmanski, e leia um resumo a respeito dos conjuntos numéricos e suas propriedades, o que pode contribuir para possíveis comparações entre esses conjuntos numéricos. Disponível em: <http://anhanguera.bv3.digitalpages.com.br/users/publications/9788559722031/pages/-2>. Acesso em: 13 abr. 2018.

Divisibilidade no conjunto de números inteiros

Verificamos anteriormente a possibilidade de definir as operações usuais de adição, multiplicação e subtração sobre o conjunto de números inteiros. Para que possamos analisar a quarta operação, a divisão, definida sobre $\mathbb{Z}$, iniciaremos pelo estudo da relação de divisibilidade sobre esse conjunto.

O número $a \in \mathbb{Z}$ é divisor de $b \in \mathbb{Z}$ (ou *a* divide *b*) se existir $c \in \mathbb{Z}$ tal que $b = ac$. Nesse caso, podemos dizer que *b* é divisível por *a* ou que *b* é múltiplo de a, adotando a notação $a \mid b$. Por exemplo, -3 divide 12 porque $12 = (-3)(-4)$.

Se $a \mid b$ e $a \neq 0$, o inteiro c tal que $b = ac$ pode ser indicado por b/a e é chamado de quociente de b por a.

Assimile

A relação de divisibilidade em $\mathbb{Z}$ goza das seguintes propriedades:

- Reflexiva: $a \mid a$ para todo $a \in \mathbb{Z}$;
- Se $a, b \geq 0$ com $a, b \in \mathbb{Z}$, $a \mid b$ e $b \mid a$, então $a = b$;
- Transitiva: se $a \mid b$ e $b \mid c$ então $a \mid c$, para todos $a, b, c \in \mathbb{Z}$;
- Se $a, b, c \in \mathbb{Z}$ tais que $a \mid b$ e $a \mid c$, então $a \mid (bx + cy)$, para quaisquer $x, y \in \mathbb{Z}$;
- Se $a \mid b$ e $c \mid d$ então $ac \mid bd$, para todos $a, b, c, d \in \mathbb{Z}$.

Analise as propriedades apresentadas e reflita sobre as justificativas que podem ser apresentadas para validar cada uma delas.

Com base na relação de divisibilidade, podemos construir o algoritmo da divisão para o conjunto de números inteiros.

O **algoritmo da divisão**, associado à operação de divisão no conjunto dos números inteiros, afirma que ao tomar os inteiros a e b, com $a > 0$, existe um único par de inteiros q e r tais que $b = aq + r$, de modo que $0 \leq r < a$. Neste caso, q é chamado de quociente e r o resto da divisão de b por a.

Exemplificando

Sejam os inteiros -17 e 3. Observe que $-17 = 3(-6) + 1$, então pelo algoritmo euclidiano, o quociente da divisão de -17 por 3 é $q = -6$ e o resto, $r = 1$.

Sendo assim, na aplicação do algoritmo da divisão considerando a divisão do número inteiro b por a é imprescindível que o resto r seja tal que $0 \leq r < a$. Esta condição deve ser satisfeita além do fato de $a > 0$.

Faça você mesmo

Determine o quociente e o resto obtidos ao aplicar o algoritmo da divisão de inteiros considerando a divisão de b por a nos seguintes casos:

(a) $b = 12$ e $a = 5$;

(b) $b = -23$ e $a = 7$.

Máximo divisor comum e mínimo múltiplo comum

Considerando a relação de divisibilidade envolvendo os números inteiros, podemos estudar também o máximo divisor comum associado a esse conjunto numérico, o qual é abordado na Educação Básica e que contribui, por exemplo, para a identificação de frações equivalentes.

A partir de $a, b \in \mathbb{Z}$ não simultaneamente nulos, o **máximo divisor comum** (*mdc*) de *a* e *b*, denotado por (a, b), é o maior inteiro *d* tal que $d \mid a$ e $d \mid b$, ou seja, o maior inteiro que divide *a* e *b* ao mesmo tempo. Assim, o inteiro (a, b) é tal que:

- (a, b) é um divisor comum de *a* e *b*;
- (a, b) é divisível por todo divisor comum de *a* e *b*.

Considere, por exemplo, os números inteiros 20 e 24. Note que 20 admite os divisores 1, 2, 4, 5, 10 e 20, enquanto que 24 admite os divisores 1, 2, 3, 4, 6, 8, 12 e 24. Observe que o maior número que divide 20 e 24 ao mesmo tempo é o 4, logo, o máximo divisor comum de 20 e 24 é 4, isto é, $(20, 24) = 4$.

Além do máximo divisor comum, podemos estudar o mínimo múltiplo comum, que corresponde a um conceito aplicado na Educação Básica, por exemplo, quando desejamos identificar frações equivalentes para aplicar as operações de adição e subtração envolvendo frações, assim como o *mdc*.

O **mínimo múltiplo comum** (*mmc*) associado a dois inteiros positivos *a* e *b* corresponde ao menor inteiro positivo simultaneamente múltiplo de *a* e *b*, o qual pode ser denotado por $[a, b]$. Este inteiro goza das seguintes propriedades:

- $[a, b]$ é um múltiplo comum de *a* e *b*;

- Se c é um múltiplo comum de a e b, então $[a,b]$ é um divisor de c.

Por exemplo, considerando os números 3 e 4, temos que o menor inteiro múltiplo de 3 e 4 simultaneamente é o 12, o qual corresponde ao mínimo múltiplo comum de 3 e 4. Veja que 24 é também um múltiplo de 3 e de 4, sendo o mesmo divisível por 12.

Para auxiliar na identificação do mínimo múltiplo comum associado a um conjunto de inteiros positivos podemos empregar a decomposição em fatores primos.

Um número natural (ou inteiro positivo) é chamado de **número primo** quando possuir exatamente dois divisores: o número 1 e ele mesmo. Caso contrário, o número é denominado composto. O conjunto de números primos pode ser descrito como $\{2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ ...\}$.

Como exemplos temos o 2, que é divisível por 1 e por 2, e o número 5, divisível por 1 e 5, sendo ambos números primos. Por outro lado, o 6 é um número composto porque, além de ser divisível por 1 e por 6, é também divisível por 2 e por 3.

Os números compostos podem ser decompostos como o produto de números primos, fato garantido pelo **Teorema Fundamental da Aritmética**, o qual afirma que todo inteiro positivo maior que 1 pode ser representado de modo único (a menos da ordem) como um produto de fatores primos. Por exemplo, podemos expressar $10 = 2 \cdot 5$, sendo 2 e 5 números primos.

Para fatorar um número composto podemos empregar as sucessivas divisões do mesmo por números primos, partindo dos menores para os maiores primos em função do número estudado.

Por exemplo, para fatorar o número 105 teremos

$$\begin{array}{r|l} 105 & 3 \\ 35 & 5 \\ 4 & 7 \\ 1 & 3 \cdot 5 \cdot 7 \end{array}$$

Logo, $105 = 3 \cdot 5 \cdot 7$. Observe que a divisão teve início pelo 3 por se tratar do menor número primo que divide o 105. Empregaremos esse mesmo processo para identificar o mínimo múltiplo comum envolvendo um conjunto de inteiros positivos.

Exemplificando

Desejamos identificar o mínimo múltiplo comum envolvendo os inteiros positivos 8, 10 e 12. Para isso, vamos decompor os três números simultaneamente em fatores primos. Iniciamos com a divisão dos números por 2, pois todos são pares, obtendo assim,

$$\begin{array}{ccc|c} 8 & 10 & 12 & 2 \\ 4 & 5 & 6 & \end{array}$$

Novamente podemos dividir os resultados por 2 porque, apesar de 5 não ser divisível por 2, os números 4 e 6 o são, assim

$$\begin{array}{ccc|c} 8 & 10 & 12 & 2 \\ 4 & 5 & 6 & 2 \\ 2 & 5 & 3 & \end{array}$$

O número 5 foi repetido da segunda para a terceira linha porque ele não é divisível por 2. Prosseguindo, como um dos resultados obtidos ainda é divisível por 2, efetuamos novamente essa divisão, e assim,

$$\begin{array}{ccc|c} 8 & 10 & 12 & 2 \\ 4 & 5 & 6 & 2 \\ 2 & 5 & 3 & 2 \\ 1 & 5 & 3 & \end{array}$$

Dentre os resultados, temos um valor múltiplo de 3, então segue que

$$\begin{array}{ccc|c} 8 & 10 & 12 & 2 \\ 4 & 5 & 6 & 2 \\ 2 & 5 & 3 & 2 \\ 1 & 5 & 3 & 3 \\ 1 & 5 & 1 & \end{array}$$

Por fim, efetuando a divisão por 5 tem-se

$$\begin{array}{ccc|l} 8 & 10 & 12 & 2 \\ 4 & 5 & 6 & 2 \\ 2 & 5 & 3 & 2 \\ 1 & 5 & 3 & 3 \\ 1 & 5 & 1 & 5 \\ 1 & 1 & 1 & 2\cdot 2\cdot 2\cdot 3\cdot 5 \end{array}$$

Como obtivemos todos os resultados, na última linha, iguais a 1, podemos encerrar o processo e efetuar, na última linha da última coluna o produto entre todos os fatores primos envolvidos, como apresentado anteriormente. Do produto de todos os fatores primos envolvidos nas divisões obtemos $2\cdot 2\cdot 2\cdot 3\cdot 5 = 120$. Portanto, o mínimo múltiplo comum de 8, 10 e 12 é 120.

Faça você mesmo

Determine o máximo divisor comum e o mínimo múltiplo comum relativo aos números 20, 35 e 48.

Pesquise mais

Para contribuir com os estudos a respeito do máximo divisor comum e do mínimo múltiplo comum, acesse a dissertação intitulada "Máximo Divisor Comum e Mínimo Múltiplo Comum Generalizados Aplicados no Ensino Básico", de Juliana de Oliveira Fiorelli, a qual investiga os fundamentos desses conceitos, refletindo sobre o ensino destes na Educação Básica. Disponível em: <http://repositorio.unicamp.br/bitstream/REPOSIP/325524/1/Fiorelli_JulianaDeOliveira_MP.pdf>. Acesso em: 13 abr. 2018.

Sem medo de errar

Para finalizar o atendimento à empresa do ramo da construção civil, sua tarefa, em conjunto com seus funcionários, será a de

identificar as numerações das casas de um condomínio horizontal, considerando uma nova estratégia adotada pela empresa.

A estratégia adotada para a determinação destas numerações deve ser avaliada para a primeira rua do empreendimento, na qual existem seis casas cujas numerações devem ser dadas da seguinte forma:

$\frac{z}{6}, \frac{z}{5}, \frac{z}{4}, \frac{z}{3}, \frac{z}{2}, z$ e nesta ordem, sabendo que z é um número inteiro e, além disso, z é o menor inteiro positivo para o qual todos os números apresentados são inteiros. Estes números ainda podem ser representados como $\frac{z}{6}, \frac{z}{5}, \frac{z}{4}, \frac{z}{3}, \frac{z}{2}, \frac{z}{1}$

Como z é o menor inteiro positivo para o qual $\frac{z}{6}, \frac{z}{5}, \frac{z}{4}, \frac{z}{3}, \frac{z}{2}, \frac{z}{1}$ sejam inteiros, devemos ter que o número z seja o mínimo múltiplo comum entre 1, 2, 3, 4, 5 e 6, porque se isso ocorrer, z será divisível por 1, 2, 3, 4, 5 e 6 e, assim, todas as razões representarão números inteiros positivos.

Vamos construir os conjuntos compostos pelos múltiplos de 1, 2, 3, 4, 5 e 6 denotados, respectivamente, por M_1, M_2, M_3, M_4, M_5 e M_6. Assim, segue que:

$$M_1 = \{1, 2, 3, 4, 5, ..., 59, 60, ...\}$$
$$M_2 = \{2, 4, 6, 8, 10, ..., 58, 60, ...\}$$
$$M_3 = \{3, 6, 9, 12, 15, ..., 57, 60, ...\}$$
$$M_4 = \{4, 8, 12, 16, 20, ..., 56, 60, ...\}$$
$$M_5 = \{5, 10, 15, 20, 25, ..., 55, 60, ...\}$$
$$M_6 = \{6, 12, 18, 24, 30, 36, 42, 48, 54, 60, ...\}$$

Analisando todos os elementos dos conjuntos apresentados, o menor inteiro que pertence a todos os conjuntos em estudo é o 60. Logo, o mínimo múltiplo comum de 1, 2, 3, 4, 5 e 6 é 60.

Outra forma para determinação do mínimo múltiplo comum é a partir da decomposição simultânea dos números envolvidos em fatores primos. Veja que:

$$\begin{array}{cccccc|l} 1 & 2 & 3 & 4 & 5 & 6 & 2 \\ 1 & 1 & 3 & 2 & 5 & 3 & 2 \\ 1 & 1 & 3 & 1 & 5 & 3 & 3 \\ 1 & 1 & 1 & 1 & 5 & 1 & 5 \\ 1 & 1 & 1 & 1 & 1 & 1 & \overline{2\cdot 2\cdot 3\cdot 5} \end{array}$$

Como $2\cdot 2\cdot 3\cdot 5 = 60$ então o mínimo múltiplo comum de 1, 2, 3, 4, 5 e 6 é igual a 60.

Assim, empregando qualquer um dos métodos apresentados, podemos observar que $z = 60$.

Sendo assim,

$$\frac{60}{6} = 10;\ \frac{60}{5} = 12;\ \frac{60}{4} = 15;\ \frac{60}{3} = 20;\ \frac{60}{2} = 30;\ \frac{60}{1} = 60$$

Desta forma, as numerações das seis casas localizadas na primeira rua do condomínio serão 10, 12, 15, 20, 30 e 60, nesta ordem.

Após a resolução desse problema, você deve elaborar um roteiro de instruções descrevendo como as numerações foram obtidas, tomando por base o conceito de mínimo múltiplo comum e as decomposições em fatores primos. Assim, organize essas informações, construindo um passo a passo de modo que este procedimento possa ser aplicado em outras situações, considerando, por exemplo, o caso geral no qual as numerações satisfaçam a condição de que as razões $\frac{z}{a}, \frac{z}{b}, \frac{z}{c}, \frac{z}{d}, \frac{z}{e}, \frac{z}{f}$ forneçam números inteiros, com $a,b,c,d,e,f \in \mathbb{Z}_+^*$.

Finalizando a proposta de estudo da unidade, construa um relatório com todas as informações coletadas e analisadas ao longo das três seções de forma sintética e que atenda a todas as necessidades apresentadas pela empresa de construção civil atendida pelo escritório. Seja objetivo nas análises e utilize, sempre que possível, recursos visuais para auxiliar na interpretação dos dados analisados durante o processo. Com isso, concluímos o atendimento à empresa do ramo da construção civil.

Avançando na prática

Aplicação da divisibilidade na resolução de problemas

Descrição da situação-problema

Na escola de Educação Básica em que você atua está sendo organizada uma Feira de Ciências. Você e o professor da disciplina de Ciências ficaram responsáveis por auxiliar os alunos de uma das turmas na organização dos trabalhos cujo tema é a Astronomia. Para isso, vocês organizaram os alunos em pequenos grupos para explorar diferentes tópicos da área apresentada.

Um dos grupos pretende elaborar um trabalho a respeito dos cometas e, para isso, desejam investigar alguns cometas específicos e os períodos de aproximação com o planeta Terra ao longo da história. Para auxiliar este grupo nos estudos, você propôs a eles o seguinte problema:

De acordo com estudos da astronomia, sabe-se que alguns cometas se aproximam da Terra periodicamente, o que possibilita prever em quais anos estes fenômenos ocorrerão. Considere que um pesquisador identificou que o cometa Z se aproxima do planeta a cada 16 anos, enquanto que o cometa W tem sua aproximação à Terra observada a cada 36 anos, cada um de forma independente um do outro. Sabendo que os cometas Z e W tiveram sua última aproximação à Terra, juntos, ocorrida em 1915, quando estes cometas passarão juntos pelo planeta novamente?

Como os alunos poderiam resolver esse problema? Proponha uma solução para o problema apresentado, identificando os conceitos que devem ser aplicados pelos alunos na resolução e as possíveis dúvidas que possam surgir ao longo de sua resolução.

Resolução da situação-problema

Como os períodos de aproximação dos cometas Z e W ao planeta Terra se dá, respectivamente, em períodos de 16 e 36 anos, para determinar em que instante os dois se aproximarão da Terra juntos é preciso identificar o mínimo múltiplo comum entre 16 e 36. Note que

$$\begin{array}{cc|l} 16 & 36 & 2 \\ 8 & 18 & 2 \\ 4 & 9 & 2 \\ 2 & 9 & 2 \\ 1 & 9 & 3 \\ 1 & 3 & 3 \\ 1 & 1 & \overline{2\cdot 2\cdot 2\cdot 2\cdot 3\cdot 3 = 144} \end{array}$$

Logo, o mínimo múltiplo comum entre 16 e 36 é igual a 144.

Se a última passagem dos dois cometas pelo planeta ocorreu em 1915 então

$$1915 + 144 = 2059$$

Portanto, a próxima passagem dois cometas, juntos, pela Terra ocorrerá em 2059

Assim, para a resolução deste problema, os alunos precisam ter conhecimentos a respeito dos conjuntos numéricos, principalmente dos inteiros, e da identificação do mínimo múltiplo comum. Existem outros métodos que podem ser empregados na resolução deste problema? Quais dúvidas poderiam ser manifestadas pelos alunos durante a resolução deste problema? Quais encaminhamentos poderiam ser adotados para auxiliar os alunos na superação das dificuldades apresentadas? Reflita a respeito destas questões e organize um plano de aula com base na questão proposta.

Faça valer a pena

1. O estudo dos conjuntos numéricos é realizado na Educação Básica considerando as propriedades dos números pertencentes a cada um dos conjuntos, as operações e propriedades associadas, voltado à resolução de problemas que exijam o emprego dessas estruturas.

Considerando as propriedades dos conjuntos numéricos e as relações de inclusão que podem ser avaliadas, complete as lacunas das seguintes afirmações, tornando-as válidas:

I. Todo número _____ pode ser classificado como um número racional.

II. Todo número _____ pode ser classificado como um número real.
III. Existem números _____ que podem ser classificados como irracionais.
IV. Existem números _____ que podem ser classificados como inteiros.

Assinale a alternativa que indica os termos que completam corretamente as lacunas das afirmações apresentadas:

a) I – real; II – racional; III – inteiros; IV – racionais.
b) I – natural; II – inteiro; III – naturais; IV – irracionais.
c) I – natural; II – racional; III – reais; IV – racionais.
d) I – inteiro; II – racional; III – naturais; IV – racionais.
e) I – inteiro; II – irracional; III – racionais; IV – naturais.

2. O estudo da divisibilidade de números inteiros possibilita, dentre outros, aplicar o algoritmo da divisão na interpretação de situações-problema que estejam relacionadas ao conjunto dos números inteiros.

A respeito desse tema, analise as afirmações apresentadas a seguir, classificando-as como verdadeiras (V) ou falsas (F):

( ) Ao dividirmos o número 12 por 7 obtemos, pelo algoritmo da divisão, o quociente 1 e o resto 5.
( ) Ao dividirmos o número -19 por 4 obtemos, pelo algoritmo da divisão, o quociente -4 e o resto -3.
( ) Ao dividirmos o número 25 por -7 obtemos, pelo algoritmo da divisão, o quociente -3 e o resto 4.
( ) Ao dividirmos o número -13 por 2 obtemos, pelo algoritmo da divisão, o quociente -7 e o resto 1.

Assinale a alternativa que indica a sequência correta de classificações:

a) V – F – V – V.
b) V – F – F – V.
c) V – F – V – F.
d) F – F – V – F.
e) F – F – V – V.

3. Para a realização de uma coleta de dados a respeito das intenções de votos para as eleições estaduais, uma empresa contratou 725 funcionários temporários, dos quais 400 são homens e 325, mulheres.

Para organizar a coleta de dados em algumas regiões específicas, selecionadas por meio de um processo de construção de amostra, definiu-se a distribuição dos funcionários em equipes conforme os seguintes critérios: todas as equipes devem conter as mesmas quantidades de funcionários e em cada equipe haverá apenas pessoas de um mesmo sexo.

Com base nos critérios apresentados, se equipes distintas devem visitar regiões diferentes, qual é a menor quantidade de regiões que podem ser atendidas pelas equipes de funcionários?

a) 15.
b) 25.
c) 29.
d) 32.
e) 50.

Referências

AUBYN, A. St.; FIGUEIREDO, M. C.; LOURA, L. de; RIBEIRO, L. VIEGAS, F. **Conjuntos**. Disponível em: <https://www.math.tecnico.ulisboa.pt/~fteix/CI/conjuntos.pdf>. Acesso em: 2 abr. 2018.

BOYER, C. B. **História da Matemática**. Tradução de Elza F. Gomide. São Paulo: Edgard Blücher, 1974.

COCHMANSKI, J. C.; COCHMANSKI, L. C. de C. **Estruturas Algébricas**. Curitiba: InterSaberes, 2016.

DOMINGUES, H. H.; IEZZI, G. **Álgebra Moderna**. São Paulo: Atual, 2003.

GARCIA, A.; LEQUAIN, Y. **Elementos de Álgebra**. Rio de janeiro: IMPA, 2015.

HEFEZ, Abramo. **Curso de Álgebra**. v. 1. Rio de Janeiro: IMPA, 2014.

PEREIRA, R. M. M.; SODRÉ, U. **Ensino Médio**: Teoria dos Conjuntos. Disponível em: <http://www.uel.br/projetos/matessencial/medio/conjuntos/conjunto.htm>. Acesso em: 2 abr. 2018.

POOLE, D. **Álgebra Linear**: uma introdução moderna. 2 ed. São Paulo: Cengage Learning, 2016.

RESENDE, M. R.; MACHADO, S. D. A. O ensino de matemática na licenciatura: a disciplina de Teoria Elementar dos Números. **Educação Matemática Pesquisa**, São Paulo, v. 14, n. 2, p. 257-278, 2012.

ROQUE, T. **História da Matemática**. Rio de Janeiro: Zahar, 2012.

ROSA, C. P. da; RIBAS, L. C.; BARAZZUTTI, M. Análise de livros didáticos. In: III Escola de Inverno de Educação Matemática, 1, 2012. Santa Maria, **Anais...** Santa Maria: UFSM, 2012. Disponível em: <http://w3.ufsm.br/ceem/eiemat/Anais/arquivos/RE/RE_2_Rosa_Carine_Pedroso.pdf>. Acesso em: 2 abr. 2018.

SANTOS, J. P. de O. **Introdução à Teoria dos Números**. Rio de Janeiro: IMPA, 2015.

STEWART, J. **Cálculo**. Volume 1. São Paulo: Cengage Learning, 2013.

VIEIRA, A. C. **Fundamentos de Álgebra I**. Belo Horizonte: Editora UFMG, 2011.

WALL, E. S. **Teoria dos Números para professores do ensino fundamental**. Porto Alegre: AMGH, 2014.

Estruturas algébricas: grupos

Convite ao estudo

Na primeira unidade deste livro foi discutido a respeito de tópicos da Teoria de Conjuntos e da Teoria dos Números, observando a aplicabilidade dos conceitos em situações envolvendo análise de dados, estudo de relações entre números a partir do mínimo múltiplo comum, entre outros. Também foi tratado sobre as operações binárias e suas propriedades.

Na presente seção estudaremos a estrutura de grupos, observando suas principais propriedades e exemplos importantes para o estudo da Álgebra, como os grupos baseados em conjuntos numéricos, grupos de simetrias e de permutações. Para que a estrutura em questão possa ser definida, precisamos considerar operações binárias e verificar as propriedades que são gozadas, conforme já estudado na unidade anterior.

Dentre as aplicações deste conteúdo, observamos que os grupos estão presentes em diversas áreas da Matemática, como a Análise Combinatória e a Física Matemática, além de outras áreas, como a Química e Física. Na Educação Básica, o estudo dos polinômios, das funções e das equações, por exemplo, toma por base as estruturas de grupos formadas a partir dos conjuntos numéricos, o que indica a importância do estudo e da compreensão desse tema.

Considere que você atua como professor de Matemática em uma escola da Educação Básica. Para dar início ao ano letivo, a instituição propôs um curso de formação continuada a todos os professores, direcionando temas específicos para cada área. Durante os três dias de curso, os professores de Matemática

da escola devem reunir-se para discutir sobre questionamentos apresentados pelos alunos, aprofundando seus estudos em relação aos conteúdos abordados nos anos finais do Ensino Fundamental e do Ensino Médio. É importante que o professor tenha conhecimentos específicos sobre os fundamentos dos conteúdos que são abordados na Educação Básica para que possa auxiliar os alunos na superação de suas dificuldades e na construção dos conhecimentos necessários à sua formação.

No primeiro dia de curso você precisará desenvolver tarefas voltadas ao estudo das propriedades satisfeitas em conjuntos numéricos, principalmente o conjunto de números inteiros, com operações correspondentes. No segundo dia você deverá estudar outros tipos de conjuntos que, em associação com operações específicas, podem ser classificados como grupos. Por fim, no último dia do curso, você precisará investigar os subgrupos e resolver um problema com base nos conhecimentos construídos ao longo do curso. Ao final dessa capacitação você deverá organizar um relatório contendo as reflexões realizadas durante os três dias, bem como justificativas a respeito da importância do estudo da teoria de grupos pelo professor como forma de contribuir na organização de propostas de trabalho envolvendo a sistematização dos conjuntos numéricos na Educação Básica.

Para cumprir o desafio proposto, na Seção 2.1, você estudará a definição de grupo e suas propriedades correspondentes, na segunda seção, os estudos serão direcionados aos exemplos importantes de grupos, como os relacionados aos conjuntos numéricos, os grupos finitos, os grupos de simetria, entre outros. Finalmente, na Seção 2.3 os estudos devem ser direcionados aos subgrupos e aos grupos de permutações. Verifique, na sequência, quais reflexões precisam ser realizadas por você durante o curso de formação continuada propostas pela instituição.

Seção 2.1

Caracterização da estrutura de grupo

Diálogo aberto

Iniciaremos agora os estudos de uma das principais estruturas algébricas: os grupos. Quando resolvemos equações polinomiais ou construímos funções tomando por base o conjunto de números reais, por exemplo, muitas das propriedades aplicadas são derivadas dos grupos que podem ser compostos a partir de $\mathbb{R}$ e suas operações. Assim, o estudo dessa estrutura é essencial para que possamos compreender os conceitos que estão envolvidos.

Portanto, com base no contexto de formação continuada proposto pela escola de Educação Básica na qual você atua, no primeiro dia do curso de formação os professores de Matemática devem direcionar seus estudos e discussões para o tema conjuntos numéricos.

Os conjuntos numéricos, principalmente dos números naturais, é trabalhado nas escolas desde a Educação Infantil. O conhecimento desses conjuntos é essencial para que os alunos possam compreender as diversas situações nas quais o emprego dos números se faz necessário, possibilitando a interpretação das situações que podem ser representadas numericamente.

Refletindo sobre este tema, principalmente em relação às propriedades presentes nos conjuntos numéricos, no primeiro dia de curso você ficou responsável por partir dos seguintes tópicos e iniciar as discussões sobre a importância da teoria de grupos para a formação de professores:

- Muitos alunos apresentam dificuldades no estudo do conjunto dos números inteiros devido à existência dos números negativos. Quais são as vantagens na resolução de problemas empregando o conjunto dos números inteiros ao invés dos naturais? Reflita sobre este tema, analisando a solução para a equação de 1º grau $x + a = b$, onde a e b são números naturais e, consequentemente, números inteiros. De que forma o conhecimento da estrutura de grupos pode auxiliar o professor a organizar o trabalho de modo

a favorecer a aprendizagem dos alunos em relação aos números inteiros?

- Outra dificuldade comum aos alunos da Educação Básica diz respeito à operação de divisão envolvendo números reais. Que relações podem ser estabelecidas entre as operações de multiplicação e divisão no conjunto numérico citado? As propriedades válidas para estas operações no conjunto dos números reais também são observadas para os números inteiros e suas operações correspondentes? Reflita sobre estas questões analisando o processo de obtenção da solução para a equação de 1º grau $ax + b = c$, onde a, b e c são números inteiros e, consequentemente, reais.

Que respostas podem ser propostas a cada uma das questões apresentadas? Que conhecimentos matemáticos fundamentam cada um dos questionamentos propostos? Quais estruturas algébricas estão associadas a cada uma das dificuldades apresentadas? Qual a importância do conhecimento da estrutura de grupos para o trabalho com os conjuntos numéricos na Educação Básica?

Analise os conteúdos necessários para a resolução destes problemas e construa um breve texto apresentando as respostas e a justificativa teórica para cada questionamento abordado, destacando aspectos relevantes a serem discutidos com os demais docentes sobre a presença da estrutura de grupos nos conteúdos trabalhados na Educação Básica. Finalize seu texto justificando por que o conjunto dos números inteiros, com a adição usual, constitui um grupo abeliano e se esse fato também pode ser observado quando tomamos a multiplicação usual.

Não pode faltar

Para o estudo das estruturas algébricas é necessário considerar os tópicos de Teoria dos Conjuntos e Teoria dos Números abordados na unidade anterior, principalmente as definições de conjuntos e operações binárias. Um dos principais objetivos com o estudo destas estruturas é generalizar padrões observados a partir de diferentes conjuntos com operações, observando as propriedades comuns. O estudo dessas estruturas pode contribuir, por exemplo, com a resolução de problemas na Educação Básica devido às propriedades observadas nos conjuntos numéricos.

Estrutura algébrica

Uma **estrutura algébrica** corresponde a uma estrutura formada por um conjunto não vazio A e uma ou mais operações binárias definidas sobre A, as quais gozam de propriedades específicas em função da categoria em estudo. Se a estrutura é formada pelo conjunto A e por uma operação $*$, essa estrutura algébrica pode ser denotada por $(A,*)$. Por exemplo, o conjunto dos números naturais com a operação usual de adição compõe uma estrutura algébrica, que pode ser representada como $(\mathbb{N},+)$, e se considerarmos as operações usuais de adição e multiplicação definidas sobre os números reais, poderemos construir a estrutura algébrica $(\mathbb{R},+,\cdot)$.

De acordo com as propriedades que são satisfeitas, considerando conjunto com operações associadas, podemos analisar diferentes categorias de estruturas algébricas. Dentre as estruturas chamadas de elementares podemos destacar os grupoides, os semigrupos e os monoides, cujas descrições são apresentadas da seguinte forma:

- Um par $(A,*)$ é classificado como **grupoide** quando a operação $*$ gozar da propriedade do fechamento em A, isto é, se $x,y \in A$ então $x*y \in A$. $(\mathbb{Z},-)$, composto pelo conjunto de números inteiros e a subtração usual, é um grupoide, pois apenas o fechamento é verificado devido ao fato de a diferença entre números inteiros sempre resultar em um inteiro.
- Um par $(A,*)$ é classificado como **semigrupo** quando o fechamento e a associatividade forem satisfeitos para a operação $*$ sobre A. A associatividade é a condição de que $x*(y*z)=(x*y)*z$ para todos $x,y,z \in A$. Podemos destacar como exemplo o conjunto dos números naturais não nulos munido da adição usual, compondo a estrutura $(\mathbb{N}^*,+)$.
- Um par $(A,*)$ é classificado como **monoide** se o fechamento, a associatividade e a existência de elemento neutro forem satisfeitos, considerando a operação $*$ definida sobre A. Na existência de elemento devemos determinar $e \in A$ de modo que $x*e=e*x=x$ para todo $x \in A$. Como exemplo, temos a estrutura $(\mathbb{Q},\cdot)$, composta pelos números racionais e pela multiplicação usual.

Reflita

Considerando as características que definem os grupoides e semigrupos, qual operação devemos definir sobre o conjunto dos números reais para que seja possível caracterizá-lo como grupoide? E como semigrupo?

Conforme estudado na unidade anterior, existem outras propriedades que podem ser satisfeitas pelas operações binárias, possibilitando a caracterização de uma das estruturas mais importantes da álgebra: os grupos.

Estrutura de grupos

A teoria de grupos apresenta aplicações nas mais diversas áreas da Matemática, como na Topologia e na Geometria Diferencial, bem como na Física, na teoria musical, entre outras. Historicamente, o conceito de grupo foi apresentado primeiramente nos trabalhos do matemático Arthur Cayley no século XIX, a partir do qual outros matemáticos como Niels Henrik Abel, Felix Klein fizeram suas contribuições para que fosse possível alcançar o nível de desenvolvimento atual desse conhecimento na Álgebra Abstrata.

Uma estrutura algébrica $(A,*)$ é classificada como **grupo** quando as seguintes propriedades forem satisfeitas pela operação $*$ definida sobre A:

- Fechamento: para todos $x,y \in A$ é válido que $x * y \in A$.
- Associatividade: para todos $x,y,z \in A$ a igualdade $(x * y) * z = x * (y * z)$ é verificada.
- Existência de elemento neutro: existe um elemento $e \in A$ tal que $x * e = e * x = x$ para qualquer $x \in A$.
- Existência de elemento simetrizável: a todo elemento $x \in A$, existe $x' \in A$, tal que $x * x' = x' * x = e$, sendo e o elemento neutro da operação $*$ definida sobre A.

Podemos comparar a definição de grupo com as estruturas apresentadas anteriormente (grupoides, semigrupos e monoides). Por exemplo, ao comparar as definições de grupo e de semigrupo temos um grupo $(A,*)$, com A não vazio, que corresponde a um semigrupo no qual as propriedades de existência de elemento

neutro e elemento simetrizável são também satisfeitas considerando a operação $*$ sobre A. Dessa forma, podemos comparar as outras estruturas entre si, o que pode contribuir para diferenciação entre as propriedades presentes em cada estrutura.

Exemplificando

Considere o conjunto dos números reais munido das operações usuais de adição $(+)$ e multiplicação $(\cdot)$. Podemos analisar as seguintes estruturas:

- $(\mathbb{R},+)$ é classificado como grupo:

  A adição de números reais é fechada devido à soma de dois números reais resultar em um real, ou seja, se $x,y\in\mathbb{R}$, então $x+y\in\mathbb{R}$. A adição em $\mathbb{R}$ é associativa, pois $(x+y)+z=x+(y+z)$ para todos $x,y,z\in\mathbb{R}$, além de admitir $0\in\mathbb{R}$ como elemento neutro, pois $0+x=x+0=x$ para todo $x\in\mathbb{R}$. A existência de elemento simétrico é satisfeita para todo $x\in\mathbb{R}$, basta tomar o simétrico $-x\in\mathbb{R}$. Por ser um grupo composto por uma operação aditiva, dizemos que $(\mathbb{R},+)$ corresponde a um grupo aditivo.

- $(\mathbb{R}^*,\cdot)$ é classificado como grupo:

  A multiplicação de números reais é fechada, pois a cada $x,y\in\mathbb{R}$ temos $x\cdot y=xy\in\mathbb{R}$, goza da associatividade, pois é válido que $(xy)z=x(yz)$ a todos $x,y,z\in\mathbb{R}$ e admite $1\in\mathbb{R}$ como elemento neutro, porque $1\cdot x=x\cdot 1=x$ a todo $x\in\mathbb{R}$. A existência de elemento simetrizável é válida para todo $x\in\mathbb{R}^*$, basta tomar $\frac{1}{x}\in\mathbb{R}^*$. Neste caso, sendo o grupo composto por uma operação multiplicativa $(\mathbb{R}^*,\cdot)$, é chamado de grupo multiplicativo.

Assimile

Um grupo $(A,*)$ é chamado de **grupo aditivo** se a operação $*$ for de característica aditiva, e será denominado **grupo multiplicativo** quando $*$ for uma operação de caráter multiplicativo.

Seja o conjunto $\mathbb{R}^*$ munido da operação de divisão usual de números reais, compondo assim a estrutura $(\mathbb{R}^*,\div)$. Veja que esta estrutura não pode ser classificada como um grupo. A operação $\div$ não é associativa, pois, por exemplo, $16\div(8\div 2)=16\div 4=4$, $(16\div 8)\div 2=2\div 2=1$, mas

$4 \neq 1$. Como não é válida a associatividade, podemos concluir que $(\mathbb{R}^*, \div)$ não é um grupo, portanto, basta que uma das condições da definição de grupo não seja satisfeita para concluirmos que a estrutura em estudo não é um grupo. Nesse caso, o par $(\mathbb{R}^*, \div)$ será um grupoide, pois temos a validade apenas do fechamento de $\div$ em relação a $\mathbb{R}^*$.

Considere o conjunto $G = \{-1,1\} \subset \mathbb{R}$, sobre o qual é definida a operação de multiplicação usual, análoga à operação definida sobre o conjunto dos números reais. Sendo assim, afirmamos que o par $(G,\cdot)$ é um grupo multiplicativo. De fato, precisamos justificar a validade das quatro operações que caracterizam a definição de grupo. Veja que a operação de multiplicação é fechada em relação a G, pois se $a,b \in G$, então $ab \in G$, pois os produtos envolvendo os elementos de G geram apenas dois resultados: 1 e -1, os quais são elementos de G. Também temos que a multiplicação é associativa em G, ou seja, $a(bc) = (ab)c$ para todos $a,b,c \in G$, porque as seguintes expressões são válidas e correspondem a todas as combinações possíveis entre elementos de G pela associatividade:

$$(-1)\cdot((-1)\cdot(-1)) = -1 = ((-1)\cdot(-1))\cdot(-1),\ 1\cdot((-1)\cdot(-1)) = 1 = (1\cdot(-1))\cdot(-1)$$

$$1\cdot(1\cdot 1) = 1 = (1\cdot 1)\cdot 1,\ (-1)\cdot((-1)\cdot 1) = 1 = ((-1)\cdot(-1))\cdot 1$$

$$1\cdot(1\cdot(-1)) = -1 = (1\cdot 1)\cdot(-1),\ (-1)\cdot(1\cdot 1) = -1 = ((-1)\cdot 1)\cdot 1$$

$$1\cdot((-1)\cdot 1) = -1 = (1\cdot(-1))\cdot 1,\ (-1)\cdot(1\cdot(-1)) = 1 = ((-1)\cdot 1)\cdot(-1)$$

O número $1 \in G$ corresponde ao elemento neutro da multiplicação em G, pois $1\cdot x = x\cdot 1 = x$ se $x = -1$ ou $x = 1$. Para o número $1 \in G$, seu simétrico corresponde ao próprio 1, pois $1\cdot 1 = 1$, e, no caso de $-1 \in G$, seu simétrico é o número -1, pois $(-1)(-1) = 1$, assim, todos os elementos de G são simetrizáveis. Portanto, $(G,\cdot)$ é um grupo multiplicativo. Outra forma de justificar esse fato é construindo a tábua da operação de multiplicação definida sobre G, conforme a Figura 2.1, para avaliar as propriedades conforme os estudos realizados na Seção 1.2.

Figura 2.1 | Tábua da operação binária relativa ao grupo $(G,\cdot)$

·	–1	1
–1	1	–1
1	–1	1

Fonte: elaborada pela autora.

Seja a operação de potenciação definida sobre o conjunto dos números naturais e representada por $\odot$. Veja que essa operação é fechada, pois se $x, y \in \mathbb{N}$, então $x \odot y = x^y \in \mathbb{N}$. No entanto, essa operação não é associativa, visto que $2 \odot (4 \odot 3) = 2 \odot 4^3 = 2 \odot 64 = 2^{64}$ e, além disso, $(2 \odot 4) \odot 3 = 2^4 \odot 3 = (2^4)^3 = 2^{12}$, porém $2^{64} \neq 2^{12}$, por exemplo. Como uma das propriedades que compõe a definição de grupo não é satisfeita, podemos concluir que o par composto pelo conjunto dos números naturais e pela operação de potenciação, representado por $(\mathbb{N}, \odot)$, não pode ser classificado como um grupo.

Faça você mesmo

Considerando as operações usuais de adição e multiplicação, podemos construir grupos aditivos e multiplicativos com base no conjunto de números racionais? De que forma? Justifique sua resposta.

Propriedades imediatas da definição de grupo

Um grupo é definido a partir de um conjunto não vazio, de uma operação binária em conjunto com as quatro propriedades destacadas anteriormente. Devido a essa estrutura, podemos verificar a validade de algumas propriedades decorrentes da definição de grupo.

Se $(A, *)$ é um grupo, as seguintes propriedades são consequências da definição:

Propriedade 1: O elemento neutro $e \in A$ é único. Com efeito, se $e, e' \in A$ são dois elementos neutros da operação $*$ definida sobre A, então, para todo $x \in A$ são válidas as igualdades $x = e * x = x * e$ e $x = e' * x = x * e'$. Como $e \in A$, da segunda expressão temos que $e = e' * e$, e sendo $e \in A$ elemento neutro, temos $e = e' * e = e'$, isto é, $e = e'$, o que implica na unicidade do elemento neutro.

Propriedade 2: O elemento simétrico associado a cada elemento de A é único. De fato, considere $x \in A$ e sejam $y, y' \in A$ dois elementos simétricos de x em relação à operação $*$ definida sobre A. Tomando $e \in A$, elemento neutro da operação em estudo, segue da propriedade da existência de elemento simétrico a validade das expressões $x * y = y * x = e$ e $x * y' = y' * x = e$, o que implica $y = y * e = y * (x * y') = (y * x) * y' = e * y' = y'$. Logo, o elemento simétrico associado a cada $x \in A$ é único.

Propriedade 3: Se $a, b \in A$, então a equação $a * x = b$ tem uma única solução em A, a qual é dada por $x = a^{-1} * b$.

Reflita

Quais argumentos podem ser empregados na demonstração da propriedade 3? Qual a relação existente entre as propriedades 2 e 3?

Propriedade 4: Todo elemento $a \in A$ é regular em relação à operação $*$. Procure justificar esse fato com base nas informações apresentadas nesta e na unidade anterior.

No entanto, além das propriedades indicadas na definição de grupo, determinadas operações binárias ainda possuem uma outra propriedade, a comutatividade, o que possibilita o estudo de uma categoria particular de grupos, descrita no tópico a seguir.

Grupos abelianos

Quando um grupo $(A, *)$ tem a propriedade comutativa para a operação $*$ definida sobre A, dizemos que $(A, *)$ é um **grupo comutativo** ou **abeliano**. Assim, todo grupo abeliano é, em particular, um grupo, por isso todas as propriedades que compõem a definição de grupo também devem ser verificadas nesse caso, além da comutatividade.

Os grupos $(\mathbb{R}, +)$, $(\mathbb{R}^*, \cdot)$ e $(G, \cdot)$, com $G = \{-1, 1\} \subset \mathbb{R}$, os quais foram estudados anteriormente são exemplos de grupos abelianos, pois em todas as estruturas apresentadas a propriedade comutativa é satisfeita, já que as operações usuais de adição e multiplicação definidas sobre $\mathbb{R}$ são comutativas, o que também ocorre quando as restringimos a subconjuntos de $\mathbb{R}$ fechados em relação às operações citadas. No entanto, nem todos os grupos podem ser classificados como abelianos.

Faça você mesmo

Justifique a validade da propriedade comutativa nos grupos $(\mathbb{R}, +)$, $(\mathbb{R}^*, \cdot)$ e $(G, \cdot)$, com $G = \{-1, 1\} \subset \mathbb{R}$.

Exemplificando

Considere o conjunto de matrizes quadradas de ordem 2, inversíveis, com entradas reais, o qual pode ser descrito como:

$$C=\left\{K=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\middle|\ \det(K)=ad-bc\neq 0 \text{ e } a,b,c,d\in\mathbb{R}\right\}$$

Considere $\cdot$ a operação de multiplicação de matrizes definida sobre C. Veja que $(C,\cdot)$ é um grupo multiplicativo e não abeliano. De fato, a operação de multiplicação de matrizes é fechada em C, pois para as matrizes $A=(a_{ij})$ e $B=(b_{ij})$, ambas elementos de C, temos que:

$$AB=\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}\begin{pmatrix}b_{11} & b_{12}\\ b_{21} & b_{22}\end{pmatrix}=\begin{pmatrix}a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22}\\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22}\end{pmatrix}\in C$$

devido à combinação dos elementos de A e B gerar uma matriz cujas entradas são todas caracterizadas por números reais. Além disso, pelas propriedades dos determinantes, como $\det(A)=a_{11}a_{22}-a_{12}a_{21}\neq 0$ e $\det(B)=b_{11}b_{22}-b_{12}b_{21}\neq 0$, segue que $\det(AB)=\det(A)\det(B)\neq 0$.

A operação $\cdot$ é associativa, pois dadas as matrizes $P,Q,R\in C$ é sempre válido que $P(QR)=(PQ)R$, fato este que decorre da associatividade das entradas das matrizes, as quais são números reais. A matriz $I_2=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\in C$ corresponde ao elemento neutro da multiplicação de matrizes, pois para toda $A\in C$ é válido que $AI_2=I_2A=A$. Como toda matriz $A\in C$ é tal que $\det(A)\neq 0$, então A admite uma inversa A^{-1} com $AA^{-1}=A^{-1}A=I_2$, o que implica que todo elemento do conjunto C é simetrizável em relação à operação de multiplicação de matrizes. Logo, considerando as justificativas apresentadas, $(C,\cdot)$ é um grupo multiplicativo. No entanto, note que a multiplicação de matrizes não é comutativa. Com efeito, sejam as matrizes $R=\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}$ e $S=\begin{pmatrix}2 & 3\\ 5 & -1\end{pmatrix}$ pertencentes a C, pois suas entradas são números reais, tais que $\det(R)=-2$ e $\det(S)=-17$. Dessa forma,

$$RS=\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}\begin{pmatrix}2 & 3\\ 5 & -1\end{pmatrix}=\begin{pmatrix}12 & 1\\ 26 & 5\end{pmatrix}$$

$$SR=\begin{pmatrix}2 & 3\\ 5 & -1\end{pmatrix}\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}=\begin{pmatrix}11 & 16\\ 2 & 6\end{pmatrix}$$

mas $RS\neq SR$. Assim, a multiplicação de matrizes não é comutativa. Portanto, $(C,\cdot)$ é um grupo multiplicativo não abeliano.

Além dos grupos definidos sobre conjuntos numéricos ou conjuntos de matrizes, podemos também estudar os grupos envolvendo outros conjuntos, como os de funções, conforme apresentado a seguir.

Considere o conjunto $F(\mathbb{R})$ composto por todas as funções reais, como é o caso da função $f:\mathbb{R}\to\mathbb{R}$ por exemplo. Definamos

a operação de adição de funções sobre $F(\mathbb{R})$ de modo que para todos $f,g \in F(\mathbb{R})$ tenhamos $(f+g)(x)=f(x)+g(x)$ para todo $x \in \mathbb{R}$, com $f+g \in F(\mathbb{R})$. Assim, a operação de adição de funções é fechada em relação a $F(\mathbb{R})$.

Note que para todos $f,g,h \in F(\mathbb{R})$, com $x \in \mathbb{R}$, é válido que

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

Sendo assim, a adição de funções é associativa. A função nula $f(x)=0 \in F(\mathbb{R})$ corresponde ao elemento neutro da adição de funções, pois para todo $g \in F(\mathbb{R})$ e todo $x \in \mathbb{R}$ temos

$$[f+g](x)=f(x)+g(x)=0+g(x)=g(x)$$
$$[g+f](x)=g(x)+f(x)=g(x)+0=g(x),$$

o que implica na adição de funções gozarem da existência de elemento neutro. Além disso, a cada $g \in F(\mathbb{R})$ existe $-g \in F(\mathbb{R})$ de modo que

$$][g+(-g)](x)=g(x)+[-g(x)]=0$$
$$[(-g)+g](x)=[-g(x)]+g(x)=0$$

Isto é, a adição de funções satisfaz a existência de elemento simetrizável a todo elemento de $F(\mathbb{R})$. Assim, devido a esse conjunto de propriedades, podemos concluir que $(F(\mathbb{R}),+)$ é um grupo. Em conjunto com as propriedades anteriores, podemos verificar que a comutatividade também é satisfeita no conjunto em estudo, pois para todos $f,g \in F(\mathbb{R})$ e todo $x \in \mathbb{R}$ segue que

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

Portanto, $(F(\mathbb{R}),+)$ pode ser classificado como um grupo abeliano.

Assimile

Com base em um par $(A,*)$, com A não vazio e $*$ uma operação binária sobre A, podemos estudar determinadas estruturas algébricas de acordo com as propriedades que são satisfeitas para $*$, conforme a seguinte listagem:

- Grupoide: fechamento.
- Semigrupo: fechamento e associatividade.
- Monoide: fechamento, associatividade e existência de elemento neutro.
- Grupo: fechamento, associatividade, existência de elemento neutro e existência de elementos simetrizáveis.
- Grupo abeliano: fechamento, associatividade, existência de elemento neutro, existência de elementos simetrizáveis e comutatividade.

Pesquise mais

Para contribuir com os estudos a respeito dos grupos, consulte a seção 1.4.1 do livro indicado disponível em sua biblioteca virtual.

COCHMANSKI, J. C.; Cochmanski, L. C. C. **Estruturas Algébricas.** Curitiba: Intersaberes, 2016.

Procure analisar cada um dos exemplos e propriedades apresentadas no material sugerido, complementando os estudos realizados nesta seção e nas seguintes.

Sem medo de errar

No primeiro dia de curso as tarefas são voltadas ao estudo de conjuntos numéricos com suas operações e propriedades correspondentes. Sua primeira tarefa consiste em avaliar o conjunto de números inteiros com base nos dois tópicos apresentados. Dessa forma, você deve analisar os dois temas de estudo e dar início às discussões a respeito da importância da teoria de grupos para a formação de professores de Matemática.

Considere a equação de 1º grau $x + a = b$ onde a e b são números naturais. A solução desta equação corresponde ao valor assumido por x para que a equação seja válida. Porém, como os números envolvidos são todos naturais, não há como resolver esta equação, pois seria necessário considerar o elemento simétrico de a em relação

à adição de números naturais, propriedade esta que não é verificada na estrutura $(\mathbb{N},+)$. No entanto, se considerarmos a estrutura $(\mathbb{Z},+)$ como base para a resolução da equação $]\ x+a=b$, teríamos a seguinte sequência de operações para a obtenção de sua solução:

$$\begin{aligned} x+a=b &\Leftrightarrow (x+a)+(-a)=b+(-a) \\ &\Leftrightarrow x+\big(a+(-a)\big)=b-a \\ &\Leftrightarrow x+0=b-a \\ &\Leftrightarrow x=b-a \end{aligned}$$

Nesse processo, foi necessário empregar, na sequência, as seguintes propriedades da adição usual de inteiros: existência de elemento simétrico para *a*, associatividade e existência de elemento neutro. Logo, quando consideramos a estrutura $(\mathbb{N},+)$, não podemos resolver a equação apresentada, enquanto em $(\mathbb{Z},+)$ sua solução é $x=b-a$, fato justificado pela ausência da propriedade de existência de elemento simetrizável em $(\mathbb{N},+)$. A diferença observada se deve à possibilidade de caracterizar $(\mathbb{Z},+)$ como um grupo, e em particular abeliano, enquanto que $(\mathbb{N},+)$ é classificado como um monoide, não satisfazendo as condições de grupo. A estrutura $(\mathbb{Z},+)$ é um grupo abeliano porque:

- A adição de inteiros é uma operação fechada, ou seja, se $x,y\in\mathbb{Z}$ então $x+y\in\mathbb{Z}$.
- A propriedade associativa é satisfeita, pois para todos $x,y,z\in\mathbb{Z}$ é válido que $x+(y+z)=(x+y)+z$.
- O elemento neutro da adição usual de inteiros é o $0\in\mathbb{Z}$, pois para todo $x\in\mathbb{Z}$ é válido que $x+0=0+x=x$. Além disso, o elemento neutro é único, pois o $0\in\mathbb{Z}$ é o único elemento de $\mathbb{Z}$ que satisfaz a condição apresentada para todo $x\in\mathbb{Z}$.
- Todo elemento $x\in\mathbb{Z}$ é simetrizável, pois a cada $x\in\mathbb{Z}$ existe um único $-x\in\mathbb{Z}$, tal que $x+(-x)=(-x)+x=0$.
- Para quaisquer $x,y\in\mathbb{Z}$ é válida a comutatividade, isto é, $x+y=y+x$.

No conjunto de números reais podemos definir as operações usuais de multiplicação e divisão. Quando restringimos as operações à $\mathbb{R}^*$, temos que estas estão associadas entre si enquanto inversas uma da outra. A operação de divisão faz-se presente quando estudamos a propriedade da existência de elemento simetrizável em relação à multiplicação de números reais não nulos. Logo, existe uma associação entre estas duas operações. No entanto, quando avaliamos estas operações definidas

sobre $\mathbb{Z}^*$, podemos observar uma relação de inversão entre ambas, porém, nem todas as propriedades observadas em $\mathbb{R}^*$ são verificadas em $\mathbb{Z}^*$ nesse caso. Vamos analisar essa afirmação com base na equação de 1º grau na forma $ax+b=c$. Inicialmente, das propriedades observadas em $(\mathbb{Z},+)$, podemos realizar os procedimentos descritos da seguinte forma:

$$\begin{aligned} ax+b=c &\Leftrightarrow (ax+b)+(-b)=c+(-b) \\ &\Leftrightarrow ax+\big(b+(-b)\big)=c-b \\ &\Leftrightarrow ax+0=c-b \\ &\Leftrightarrow ax=c-b \end{aligned}$$

Eles envolvem a existência de elemento simetrizável, a associatividade e a existência de elemento neutro para a adição usual de inteiros, conforme observado anteriormente.

Seja agora a expressão $ax=c-b$ e a estrutura $(\mathbb{Z}^*,\cdot)$. Note que se $a\in\mathbb{Z}^*$ é tal que $a=1$ então seu simétrico será dado por $a^{-1}=1$, ou no caso em que $a=-1$, o simétrico correspondente é $a^{-1}=-1$. Porém, se $a\neq 1$ e $a\neq -1$ temos que *a* não admite simétrico em relação à multiplicação usual de inteiros não nulos, assim, não é possível partir de $ax=c-b$ para identificar *x* em função de *a*, *b* e *c*, o que impossibilita resolver a equação $ax+b=c$ em $(\mathbb{Z}^*,\cdot)$. Por outro lado, tomando a estrutura $(\mathbb{R}^*,\cdot)$ podemos empregar os seguintes procedimentos:

$$\begin{aligned} ax=c-b &\Leftrightarrow \frac{1}{a}(ax)=\frac{1}{a}(c-b) \\ &\Leftrightarrow \left(\frac{1}{a}a\right)x=\frac{1}{a}(c-b) \\ &\Leftrightarrow 1x=\frac{1}{a}(c-b) \\ &\Leftrightarrow x=\frac{1}{a}(c-b) \end{aligned}$$

Portanto, em $(\mathbb{R}^*,\cdot)$ a equação $ax+b=c$ admite a solução $x=\frac{1}{a}(c-b)$. Essa diferenciação ocorre porque $(\mathbb{Z}^*,\cdot)$ não pode ser classificado como um grupo devido à ausência da propriedade de existência de elemento simetrizável a todo $x\in\mathbb{Z}^*$. Assim, como $(\mathbb{Z}^*,\cdot)$ satisfaz apenas ao fechamento, associatividade e existência de elemento neutro, essa estrutura pode ser classificada como um monoide, enquanto $(\mathbb{R}^*,\cdot)$ pode ser classificado como um grupo abeliano. Para complementar este estudo, comprove a validade das propriedades citadas para a estrutura $(\mathbb{Z}^*,\cdot)$ de modo análogo ao que foi adotado para o estudo de $(\mathbb{Z},+)$ anteriormente.

Analisando a proposta de realização de uma discussão com os demais docentes a respeito da importância da teoria de grupos na Educação Básica, quais justificativas poderiam ser consideradas? Como você auxiliaria os demais professores de Matemática na percepção da importância da teoria de grupos, por exemplo, para a resolução das equações propostas nos dois tópicos de estudo? Construa um breve relatório indicando quais seriam os principais tópicos a serem discutidos com base nos questionamentos e no tema propostos para estudo.

Avançando na prática

A teoria de grupos e o conjunto de números complexos

Descrição da situação-problema

Você deve elaborar um plano de ensino voltado ao estudo dos Números Complexos para uma turma do Ensino Médio. Nele, você pretende preparar aulas visando introduzir os estudos a respeito do conjunto de números complexos, avaliando, dentre outros temas, a definição de i e de suas potências, bem como as operações usuais de adição e multiplicação definidas sobre esse conjunto.

Antes de elaborar o plano, você decidiu aprofundar seus estudos a respeito desse conjunto numérico lendo livros de Álgebra Abstrata, para que possa elaborar atividades adequadas aos alunos da turma em questão. Durante esses estudos, você observou a seguinte afirmação: *O conjunto* $A = \{1, -1, i, -i\} \subset \mathbb{C}$*, com a operação usual de multiplicação proveniente do conjunto* $\mathbb{C}$, corresponde a um grupo abeliano. Como você justificaria essa afirmação? De que forma as tábuas de operações podem contribuir com essa justificativa? Que relação você pode estabelecer entre o conjunto A e as potências da unidade imaginária i?

Resolução da situação-problema

Seja o conjunto $A = \{1, -1, i, -i\} \subset \mathbb{C}$ e a operação usual de multiplicação de números complexos. Assim como estudado na unidade anterior, as tábuas de operações podem ser empregadas para a obtenção mais rápida das combinações entre os elementos do conjunto a partir da operação selecionada, além de possibilitarem a identificação de propriedades que são satisfeitas na estrutura em estudo. A tábua associada à estrutura $(A, \cdot)$ é descrita conforme a Figura 2.2.

Figura 2.2 | Tábua correspondente a $(A,\cdot)$

$\cdot$	-1	1	$-i$	i
-1	1	-1	i	$-i$
1	-1	1	$-i$	i
$-i$	i	$-i$	-1	1
i	$-i$	i	1	-1

Fonte: elaborada pela autora.

Veja que a operação $\cdot$ é fechada em relação à A, pois o produto entre elementos de A pertence a esse mesmo conjunto, o que pode ser observado a partir das combinações indicadas na tábua da Figura 2.2. Além disso, a operação $\cdot$ é associativa em A, pois corresponde a uma restrição da multiplicação usual definida sobre $\mathbb{C}$ ao conjunto A, que é associativa. Assim, para quaisquer $x,y,z \in A$ temos a validade de $x+(y+z)=(x+y)+z$.

Pela tábua apresentada na Figura 2.2, podemos identificar de forma simplificada a validade de algumas das propriedades associadas à definição de grupo, conforme os seguintes itens:

- $1 \in A$ é o elemento neutro da operação, porque a linha e a coluna a que esse elemento pertence coincide, respectivamente, com a linha e a coluna fundamentais.
- todos os elementos são simetrizáveis, pois o número 1 está presente em todas as linhas e colunas, assumindo posições simétricas em relação à diagonal principal quando fixamos um elemento e analisamos sua linha e coluna correspondentes.
- a operação é comutativa porque a tábua é simétrica em relação à diagonal principal.

Portanto, podemos concluir que $(A,\cdot)$ é um grupo abeliano.

Conseguimos relacionar o conjunto A com as potências da unidade imaginária no sentido de que A destaca todos os possíveis resultados obtidos no estudo dessas potências. Isso ocorre devido às potências de i serem originadas de produtos envolvendo i como os únicos fatores e sendo a multiplicação definida sobre A ser fechada.

Após essa análise, elabore uma explicação para a turma de Ensino Médio a respeito das potências de i, tomando como base o estudo da

estrutura algébrica $(A,\cdot)$ caracterizada como grupo abeliano. Indique, de forma complementar a essa explicação, as propriedades envolvidas para o estudo das potências de *i* com base no que foi discutido anteriormente.

Faça valer a pena

1. A partir de um conjunto $P=\{a,\ b,\ c,\ d\}$, munido de uma operação $\otimes$, foi construída a tábua indicada na Figura 2.3.

Figura 2.3 |Tábua referente à estrutura $(P,\otimes)$

$\otimes$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	b	a
d	d	c	a	b

Fonte: elaborada pela autora.

A respeito dessa estrutura, foram construídas as seguintes afirmações e uma relação proposta entre elas:

I) I. A estrutura $(P,\otimes)$ pode ser classificada como um grupo.

PORQUE

II) II. Não existe a repetição de elementos nas linhas e colunas da tábua.

Em relação as afirmações apresentadas, assinale a alternativa correta:

a) As afirmações I e II estão corretas, e a II é uma justificativa correta para I.
b) As afirmações I e II estão corretas, mas a II não é uma justificativa correta para I.
c) A afirmação I está correta e a II incorreta.
d) A afirmação II está correta e a I incorreta.
e) As afirmações I e II estão incorretas.

2. Por meio do estudo da teoria de grupos podemos identificar propriedades comuns a diversas estruturas, possibilitando estabelecer relações entre diferentes conjuntos com operações a partir da identificação de padrões e regularidades.
Em relação a esse tema, analise os itens apresentados que são compostos por conjuntos não vazios e operações correspondentes.

I) Conjunto dos números inteiros negativos com a operação usual de adição $(\mathbb{Z}_-^*, +)$
II) Conjunto dos números inteiros pares $(A = \{2k \mid k \in \mathbb{Z}\})$ com a operação usual de adição $(A, +)$
III) Conjunto dos números inteiros ímpares $(B = \{2k+1 \mid k \in \mathbb{Z}\})$ com a operação usual de multiplicação $(B, \cdot)$

Considerando as informações apresentadas, assinale a alternativa correta:

a) Apenas o item II apresenta uma estrutura que pode ser classificada como grupo.
b) Apenas o item III apresenta uma estrutura que pode ser classificada como grupo.
c) Apenas os itens I e II apresentam estruturas que podem ser classificadas como grupos.
d) Apenas os itens I e III apresentam estruturas que podem ser classificadas como grupos.
e) Apenas os itens II e III apresentam estruturas que podem ser classificadas como grupos.

3. Um estudante, ao analisar um conjunto $K = \{m, n, p, q\}$ munido de uma operação Δ conveniente, verificou que a estrutura (K, Δ) pode ser classificada como um grupo abeliano.
Durante seus estudos, ele construiu uma tábua de operação associada à estrutura (K, Δ), conforme a Figura 2.4.

Figura 2.4 | Tábua associada à estrutura (K, Δ)

Δ	m	n	p	q
m	m	n	p	q
n	n	I	II	III
p	p	q	m	IV
q	q	m	n	V

Fonte: elaborada pela autora.

Para que (K, Δ) satisfaça à condição de ser um grupo abeliano, quais elementos devem ocupar as posições destacadas por I, II, III, IV e V?

a) I – q; II – n; III – m; IV – q; V – p.
b) I – n; II – m; III – q; IV – q; V – n.
c) I – p; II – m; III – n; IV – m; V – q.
d) I – m; II – n; III – q; IV – n; V – q.
e) I – p; II – q; III – m; IV – n; V – p.

Seção 2.2

Alguns exemplos importantes de grupos

Diálogo aberto

Na primeira seção desta unidade estudamos a definição de grupo, a qual depende dos conjuntos, das operações binárias e suas propriedades. Com essa definição, agora podemos analisar diversas estruturas que, apesar de envolverem elementos e operações de naturezas diferentes, apresentam um mesmo comportamento no que se refere às suas propriedades.

Dentre as diferentes estruturas de grupos, podemos destacar determinados conjuntos numéricos com suas operações correspondentes, como $\mathbb{Z}$ com a adição usual ou $\mathbb{R}^*$ com a multiplicação usual, por exemplo. A partir dessas caracterizações, estas estruturas podem ser empregadas, dentre outras aplicações, na resolução de problemas da matemática e de outras áreas, no caso em que for possível representa-los matematicamente.

No segundo dia do curso de formação continuada para professores na instituição da Educação Básica em que você atua, os professores de Matemática precisarão investigar outros conjuntos além dos numéricos.

Para esta etapa do curso, você deverá elaborar e realizar uma breve apresentação aos outros docentes do grupo, complementando os estudos realizados no primeiro dia de curso sobre os seguintes tópicos:

- Dentre os conjuntos abordados na Educação Básica, existem outros conjuntos, além dos numéricos, que também são dotados de operações e que satisfazem à estrutura de grupos. Cite ao menos dois exemplos, identificando as operações associadas e justificando as propriedades que são satisfeitas para os conjuntos descritos. Verifique também se estes conjuntos com operações podem ser classificados como grupos abelianos.
- Podemos relacionar a estrutura de grupos com a Geometria Plana por meio da construção de grupos originados de

figuras geométricas estudadas na Educação Básica. Analise as propriedades dos triângulos equiláteros e o grupo de simetria construído a partir dessa figura, evidenciando qual operação deve ser considerada e justificando por que essa estrutura pode ser classificada como um grupo.

Qual é a importância da teoria de grupos para a compreensão das questões propostas? Elabore uma descrição para cada um dos tópicos propostos, respondendo às questões apresentadas e destacando a importância da teoria de grupos para a fundamentação de cada tema presente nos tópicos para estudo. Em seguida, elabore uma breve apresentação, ressaltando a importância do conhecimento da teoria de grupos para a investigação dos temas propostos e para o ensino dos conteúdos correspondentes na Educação Básica.

Não pode faltar

Grupos associados aos conjuntos numéricos

Na seção anterior estudamos que um grupo é composto por um conjunto não vazio e por uma operação binária definida sobre o conjunto, a qual deve satisfazer as propriedades do fechamento, associativa, existência de elemento neutro e existência de elemento simetrizável. Além disso, se a propriedade comutativa for verificada, podemos classifica-la como um grupo abeliano.

Dentre os principais exemplos de estrutura de grupos, podemos destacar aquelas que derivam dos conjuntos numéricos. A seguir, vamos analisar quais os principais grupos que podem ser construídos a partir dos conjuntos numéricos. Durante essa análise, procure estudar as justificativas que podem ser empregadas na validação de cada uma das propriedades indicadas, conforme estudado na seção anterior.

- Grupo aditivo dos inteiros $(\mathbb{Z},+)$: o conjunto dos números inteiros, munido da operação usual de adição, pode ser classificado como um grupo abeliano, pois a operação de adição nesse conjunto é fechada, associativa, comutativa, o elemento neutro corresponde ao zero e a cada inteiro $a \in \mathbb{Z}$ existe o simétrico (ou oposto) correspondente à $-a \in \mathbb{Z}$.

- Grupo aditivo dos racionais $(\mathbb{Q},+)$: o conjunto dos números racionais, munido da operação usual de adição, pode ser classificado como um grupo abeliano e podemos empregar justificativas análogas ao caso de $(\mathbb{Z},+)$, adaptando-as ao conjunto $\mathbb{Q}$.
- Grupo aditivo dos reais $(\mathbb{R},+)$: o conjunto dos números reais, munido da operação usual de adição, pode ser classificado como um grupo abeliano, e podemos empregar justificativas análogas ao caso de $(\mathbb{Z},+)$, adaptando-as ao conjunto $\mathbb{R}$.
- Grupo aditivo dos complexos $(\mathbb{C},+)$: a soma de dois números complexos $z=a+bi$ e $w=c+di$ é definida como $z+w=(a+c)+(b+d)i$. Assim, essa operação de adição usual definida sobre $\mathbb{C}$ é fechada, associativa, comutativa, admite o elemento neutro $0=0+0\cdot i$ e a cada número complexo $z=a+bi$ existe o oposto $-z=-a-bi\in\mathbb{C}$. Logo, $(\mathbb{C},+)$ corresponde a um grupo abeliano.
- Grupo multiplicativo dos racionais $(\mathbb{Q}^*,\cdot)$: o conjunto dos números racionais não nulos, com a multiplicação usual, pode ser classificado como um grupo abeliano, por ser fechado e gozar das propriedades associativa, comutativa e existência de elemento neutro, que corresponde ao 1. Nós restringimos ao conjunto $\mathbb{Q}^*$, excluindo o zero, porque, nesse caso, todo elemento $a\in\mathbb{Q}^*$, isto é, todo racional não nulo *a* admite um simétrico (inverso) $a^{-1}\in\mathbb{Q}^*$, sendo a existência de elemento simetrizável válida a todo elemento de $\mathbb{Q}^*$.
- Grupo multiplicativo dos reais $(\mathbb{R}^*,\cdot)$: o conjunto dos números reais não nulos, com a multiplicação usual, pode ser classificado como um grupo abeliano, sendo as justificativas análogas ao caso do grupo $(\mathbb{Q}^*,\cdot)$.
- Grupo multiplicativo dos complexos $(\mathbb{C}^*,\cdot)$: o produto de dois números complexos $z=a+bi$ e $w=c+di$ é definido como $zw=(ac-bd)+(ad+bc)i$. Assim, essa operação de multiplicação usual definida sobre $\mathbb{C}$ é fechada, associativa, comutativa, admite o elemento neutro $1=1+0\cdot i$ e a cada número complexo não nulo $z=a+bi$, com *a* e *b* não simultaneamente nulos, existe o inverso $z^{-1}=\frac{a}{a^2+b^2}+\frac{-b}{a^2+b^2}i\in\mathbb{C}$. Desta forma, $(\mathbb{C}^*,\cdot)$ corresponde a um grupo abeliano.

Reflita

Considerando as operações usuais sobre o conjunto $\mathbb{N}$, é possível construir algum grupo com base nos elementos de $\mathbb{N}$ ou de seus subconjuntos? Identifique justificativas que fundamentem a sua resposta.

Observamos anteriormente um resumo dos principais grupos que podem ser construídos tomando por base os conjuntos numéricos. Nos casos apresentados, consideramos o conjunto numérico por completo ou excluímos o zero do conjunto, nos casos dos grupos multiplicativos. No entanto, podemos construir outros grupos em que o conjunto correspondente também seja formado por números, mas por uma quantidade limitada desses elementos, o que nos permite estudar os chamados grupos finitos.

Grupos finitos

Um **grupo finito** $(A,*)$ é uma estrutura na qual o conjunto A é não vazio e finito, ou seja, possui uma quantidade limitada de elementos. Nesse caso, podemos caracterizar a ordem do grupo, a qual corresponde ao número de elementos do conjunto A e pode ser denotada por $o(A)$. Além disso, o estudo destes tipos de grupos pode ser realizado com base na tábua de operações correspondente.

Exemplificando

Um dos principais exemplos de grupo finito que temos, associado aos conjuntos numéricos, é o grupo composto pelo conjunto $G=\{-1,\ 1\}\subset\mathbb{R}$ munido da operação usual de multiplicação definida sobre $\mathbb{R}$ e restrita a G. A tábua de operação associada a esse grupo foi apresentada na seção anterior, na Figura 2.1, e nessa mesma seção avaliamos que este grupo é abeliano. Note que o conjunto G possui dois elementos, de onde segue que o grupo $(G,\cdot)$ corresponde a um grupo finito de ordem 2, isto é, $o(G)=2$.

Outro exemplo que podemos destacar é o grupo definido a partir do conjunto $A=\{1,-1,\ i,-i\}\subset\mathbb{C}$ munido da operação usual de multiplicação de números complexos. A tábua deste grupo também foi apresentada na seção anterior, na Figura 2.2. Como $(A,\cdot)$ corresponde a um grupo, em particular abeliano, podemos concluir que $(A,\cdot)$

corresponde a um grupo finito de ordem 4, pois o conjunto *A* contém 4 elementos, e assim, $o(A) = 4$.

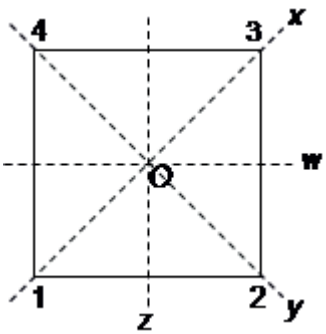
Faça você mesmo

Construa a tábua associada a um grupo finito $(P, *)$, com $P = \{a, b, c, d, e, f\}$, de ordem 6, sabendo que $(P, *)$ é abeliano. O elemento neutro do grupo é *e*, levando em conta também as seguintes relações válidas: $a * d = b * c = f$, $a * c = b * b = d$, $a * f = b * d = e$, $c * d = a$.

Grupos de simetrias

Considere um quadrado *Q* com vértices consecutivos representados por 1, 2, 3 e 4. Além disso, denote por *O* o centro de gravidade do quadrado e por *x*, *y*, *z* e *w* as retas do espaço determinadas pelas diagonais e mediatrizes do quadrado, conforme a Figura 2.5. A partir de reflexões e rotações podemos alterar as posições dos pontos e das retas que caracterizam essa figura geométrica, com base na Figura 2.5, de modo a construir as simetrias do quadrado.

Figura 2.5 | Quadrado *Q* de vértices 1, 2, 3 e 4 com diagonais e mediatrizes



Fonte: elaborada pela autora.

Denomina-se **simetria** de um quadrado *Q* qualquer aplicação bijetiva $f : Q \to Q$ que preserva distâncias, ou seja, se aplicamos a bijeção f sobre pontos *a* e *b* do quadrado, a distância entre $f(a)$ e $f(b)$ será igual à distância entre *a* e *b*. Assim, essa aplicação *f* refere-se a uma transformação que, ao ser aplicada em um quadrado, gera uma

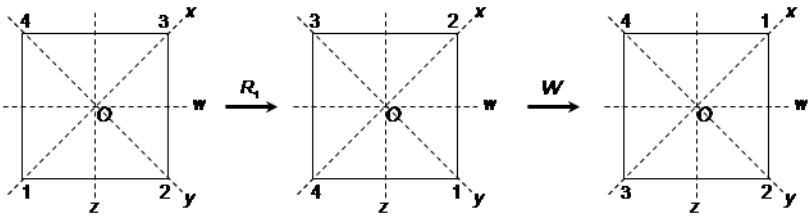
imagem que é uma cópia do quadrado inicial e coincide com este, porém, existem mudanças nos posicionamentos de seus pontos.

Vamos construir o conjunto S_4 das simetrias do quadrado. Denotemos por R_0, R_1, R_2 e R_3 as rotações avaliadas, respectivamente, segundo um ângulo de 0, $\frac{\pi}{2}$, π e $\frac{3\pi}{2}$ radianos em torno de *O*, no sentido anti-horário. Sendo assim, partindo do quadrado *Q* ilustrado na Figura 2.5, temos as seguintes transformações: $R_0 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix}$, $R_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{bmatrix}$, $R_2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix}$ e $R_3 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}$. Além disso, podemos construir as reflexões do quadrado em torno das diagonais e mediatrizes. Consideremos *X* e *Y* as reflexões de π radianos em torno das diagonais *x* e *y*, respectivamente, e *Z* e *W* as reflexões de π radianos em torno das mediatrizes *z* e *w*, respectivamente. Neste caso, com base no quadrado *Q* da Figura 2.5, teremos as transformações descritas por: $X = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{bmatrix}$, $Y = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{bmatrix}$, $Z = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}$ e $W = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix}$.

Desta forma, $S_4 = \{R_0, R_1, R_2, R_3, X, Y, Z, W\}$ corresponde ao conjunto de simetrias do quadrado. Verifique que estas são as únicas possibilidades de transformações que podem ser aplicadas sobre *Q* com base em rotações e reflexões que preservam distâncias.

Podemos aplicar uma sequência dessas transformações sobre um quadrado *Q* de modo a construir uma simetria deste. Na Figura 2.6 é apresentada a figura geométrica obtida como resultado da aplicação de R_1 e de *W*, nesta ordem, sobre o quadrado *Q* da Figura 2.5.

Figura 2.6 | Simetria de Q obtida em função das transformações R_1 e *W*



Fonte: elaborada pela autora.

A partir da Figura 2.6 podemos observar que a simetria resultante é tal que as distâncias entre os vértices do quadrado são preservadas, porque, no caso apresentado, a sucessiva aplicação de R_1 e *W* originou *Y*, que corresponde a uma simetria. Assim, a combinação entre as transformações satisfaz à condição de ser simetria. Desta forma, temos uma operação que pode ser definida a partir do conjunto S_4: a composição de transformações, que pode

ser denotada por $\circ$. Na Figura 2.7 é ilustrada a tábua da operação composição definida sobre o conjunto S_4.

Figura 2.7 | Tábua da operação $\circ$ definida sobre S_4

$\circ$	R_0	R_1	R_2	R_3	X	Y	Z	W
R_0	R_0	R_1	R_2	R_3	X	Y	Z	W
R_1	R_1	R_2	R_3	R_0	Z	W	Y	X
R_2	R_2	R_3	R_0	R_1	Y	X	W	Z
R_3	R_3	R_0	R_1	R_2	W	Z	X	Y
X	X	Z	Y	W	R_0	R_2	R_1	R_3
Y	Y	W	X	Z	R_2	R_0	R_3	R_1
Z	Z	Y	W	X	R_3	R_1	R_0	R_2
W	W	X	Z	Y	R_1	R_3	R_2	R_0

Fonte: elaborada pela autora.

Assimile

Ao analisar a tábua correspondente à estrutura, $(S_4,\circ)$, podemos observar que a composta de duas rotações corresponde a uma rotação, enquanto a composta de duas reflexões é uma rotação. Além disso, a composta de uma rotação com uma reflexão, ou vice-versa, é uma reflexão.

Temos que $(S_4,\circ)$ corresponde a um grupo. De fato, o fechamento é satisfeito para a estrutura apresentada, porque combinações entre elementos de S_4 pela composição sempre resultará em elementos desse mesmo conjunto, como observado na tábua. A composição de transformações é associativa. Como você justificaria essa afirmação?

Além disso, o elemento neutro deste grupo corresponde à R_0 porque, pela tábua da operação, a linha e coluna a que esse elemento pertence são iguais à linha e coluna fundamentais. Todos os elementos de S_4 são simetrizáveis. Note que cada uma das reflexões *X*, *Y*, *Z* e *W* é inversa de si própria, pois $X \circ X = Y \circ Y = Z \circ Z = W \circ W = R_0$. Além disso, temos que R_0 é a inversa dele próprio, assim como R_2, pois $R_0 \circ R_0 = R_0$ e $R_2 \circ R_2 = R_0$. Para as demais rotações temos $R_1 \circ R_3 = R_3 \circ R_1 = R_0$, isto é, R_1 e R_3 são inversas uma da outra.

Reflita

O grupo $(S_4, \circ)$ pode ser classificado como um grupo abeliano? Por quê?

Além dos grupos de simetrias formados a partir dos quadrados, podemos estender essa ideia para polígonos regulares quaisquer de n lados. Neste caso, se o polígono em estudo apresenta n lados, então existe uma quantidade de simetrias associadas a ele igual a $2n$. Ao compor o conjunto D_n, contendo todas as $2n$ possíveis simetrias do polígono regular com n lados, associando-o com a operação de composição de transformações $\circ$, temos que $(D_n, \circ)$ forma um grupo, chamado de **grupo diedral de grau n**. O grupo $(S_4, \circ)$ que estudamos, envolvendo as simetrias do quadrado, corresponde ao grupo diedral de grau 4.

Pesquise mais

Para complementar os estudos a respeito dos grupos de simetrias, estude o capítulo 4 da dissertação indicada. Neste mesmo trabalho, no capitulo 5, você pode conferir uma análise dos grupos de simetrias construídos a partir de figuras tridimensionais.

REIS, Elisandra Regina Sampaio dos. **Estudo de simetria e seu ensino no nível fundamental e médio**. 2013, 58 f. Dissertação (Mestrado Profissional em Matemática) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Paulo. Disponível em: <http://www.teses.usp.br/teses/disponiveis/55/55136/tde-12112013-164400/publico/Elisandra_revisada.pdf>. Acesso em: 13 jul. 2018.

Além dos grupos construídos com base nos conjuntos numéricos, os grupos de simetrias, temos ainda os grupos de classes de resto, os quais são construídos a partir do conjunto de números inteiros e da relação de divisibilidade definida sobre este.

Outros grupos importantes

Vamos considerar o conjunto $\mathbb{Z}$ e o algoritmo da divisão associado a ele. Por exemplo, quando dividimos qualquer número inteiro por 3, os únicos restos possíveis da divisão são 0, 1 e 2, conforme as

condições associadas ao algoritmo da divisão. Podemos construir as classes de resto associadas a essas divisões, ou seja, os conjuntos formados pelos inteiros que apresentam o mesmo resto ao serem divididos por 3. Neste caso, teremos as classes $\bar{0} = \{..., -6, -3, 0, 3, 6, ...\}$, $\bar{1} = \{..., -5, -2, 1, 4, 7, ...\}$ e $\bar{2} = \{..., -4, -1, 2, 5, 8, ...\}$.

Note que todos os números que pertencem a uma mesma classe geram o mesmo resto ao serem divididos por 3. Assim, temos o conjunto $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$, chamado de conjunto das classes de resto módulo 3, por se tratar da divisão pelo inteiro 3. Podemos definir duas operações sobre esse conjunto: a adição, na qual para $\bar{a}, \bar{b} \in \mathbb{Z}_3$ tem-se $\bar{a} + \bar{b} = \overline{a+b}$, e a multiplicação, onde se $\bar{a}, \bar{b} \in \mathbb{Z}_3$, então $\bar{a} \cdot \bar{b} = \overline{a \cdot b} = \overline{ab}$.

Considerando a estrutura $(\mathbb{Z}_3, +)$, temos que as propriedades do fechamento, associativa e comutativa são válidas. O elemento neutro da adição corresponde a $\bar{0}$, enquanto a classe $\overline{3-a}$ corresponde ao oposto de $\bar{a} \in \mathbb{Z}_3$. Portanto, $(\mathbb{Z}_3, +)$ é um grupo abeliano. Por outro lado, no caso de $(\mathbb{Z}_3^*, \cdot)$, na qual excluímos o elemento $\bar{0}$, o fechamento, a associatividade e a comutatividade são válidas. O elemento neutro da multiplicação corresponde a $\bar{1}$, enquanto todo elemento de $\mathbb{Z}_3^*$ admite o inverso. Dessa forma, $(\mathbb{Z}_3^*, \cdot)$ é um grupo abeliano. As tábuas das estruturas $(\mathbb{Z}_3, +)$ e $(\mathbb{Z}_3^*, \cdot)$ são indicadas nas Figuras 2.8(a) e 2.8(b).

Figura 2.8 | Tábuas dos grupos associados às classes de resto módulo 3

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

(a) $(\mathbb{Z}_3, +)$

·	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{2}$	$\bar{1}$

(b) $(\mathbb{Z}_3^*, \cdot)$

Fonte: elaborada pela autora.

Com base nas tábuas da Figura 2.8, justifique as propriedades que tornam as estruturas $(\mathbb{Z}_3, +)$ e $(\mathbb{Z}_3^*, \cdot)$ em grupos abelianos. Podemos ainda generalizar essa ideia para outros casos.

Assimile

Para qualquer inteiro $m > 1$, podemos construir o conjunto das classes de resto módulo m dado por $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{m-1}\}$. Definindo sobre $\mathbb{Z}_m$ a operação de adição correspondente, temos que $(\mathbb{Z}_m, +)$ é um grupo abeliano denominado **grupo aditivo das classes de resto módulo** m. Além disso, podemos definir sobre $\mathbb{Z}_m$ a operação de multiplicação. Tomando o conjunto $\mathbb{Z}_m^*$ e restringindo m a um número primo, temos que $(\mathbb{Z}_m^*, \cdot)$ pode ser classificado como um **grupo multiplicativo**. Na construção do grupo multiplicativo as considerações de $\mathbb{Z}_m^*$ e m primo são essenciais porque, no primeiro caso, o elemento $\bar{0}$ não admite inverso multiplicativo e precisa ser desconsiderado do conjunto para que este configure-se como grupo com a multiplicação, e no segundo, para que cada elemento de $\mathbb{Z}_m^*$ admita um único inverso multiplicativo.

Faça você mesmo

Estude as propriedades do grupo $(\mathbb{Z}_4, +)$ construído a partir do conjunto das classes de resto módulo 4, relacionado aos restos da divisão dos números inteiros por 4 obtidos com base no algoritmo da divisão de inteiros.

Sem medo de errar

No segundo dia do curso, a proposta é que sejam analisados outros grupos além daqueles formados a partir dos conjuntos numéricos. Você ficou responsável por estudar e elaborar uma apresentação aos demais colegas a respeito de dois tópicos, buscando ressaltar a importância do conhecimento da teoria de grupos para a formação do professor de Matemática.

Nesse sentido, a primeira parte de sua tarefa consiste em identificar exemplos de grupos derivados de conjuntos de outras naturezas, além dos numéricos, que são discutidos na Educação Básica. Para cumprir essa tarefa, um conjunto que pode ser avaliado a partir da estrutura de grupos é o conjunto de matrizes com entradas reais.

Seja o conjunto formado por todas as matrizes com entradas reais e de tamanho $m \times n$, em que m e n são números naturais, o

qual pode ser denotado por $M_{m\times n}(\mathbb{R})$. Os elementos desse conjunto assumem a seguinte forma $A=(a_{ij})$ cujas entradas a_{ij} são números reais para todos $1\leq i\leq m$ e $1\leq j\leq n$. Podemos definir a adição de matrizes como segue: se $A=(a_{ij})$, $B=(b_{ij})\in M_{m\times n}(\mathbb{R})$, isto é, são matrizes $m\times n$ com entradas reais, então a soma de *A* e *B* é dada por $A+B=(a_{ij}+b_{ij})$, a qual corresponde a uma matriz $m\times n$ com entradas reais. Logo, a adição de matrizes sobre $M_{m\times n}(\mathbb{R})$ está bem definida, satisfazendo a propriedade do fechamento.

A estrutura $(M_{m\times n}(\mathbb{R}),+)$ pode ser classificada como um grupo abeliano. De fato, o fechamento é satisfeito e, considerando matrizes $A,B,C\in M_{m\times n}(\mathbb{R})$ quaisquer, a propriedade associativa é satisfeita, pois $A+(B+C)=(A+B)+C$, bem como a comutativa, porque $A+B=B+A$. O elemento neutro da adição de matrizes é a matriz nula $m\times n$, a qual tem todas as entradas nulas e pode ser denotada por $0_{m\times n}$. A existência de elemento simetrizável é satisfeita a todo elemento de $M_{m\times n}(\mathbb{R})$, pois a cada matriz $A=(a_{ij})$ desse conjunto, podemos identificar outra matriz $-A=(-a_{ij})$ também de $M_{m\times n}(\mathbb{R})$ para a qual $A+(-A)=(a_{ij}+(-a_{ij}))=0_{m\times n}$.

Para construir um grupo multiplicativo derivado do conjunto de matrizes, precisaremos restringir $M_{m\times n}(\mathbb{R})$ a um subconjunto em que as propriedades características sejam satisfeitas. Assim, seja o conjunto composto pelas matrizes quadradas de ordem *n*, representado por $M_n(\mathbb{R})$, e, a partir deste, consideremos apenas aquelas que são inversíveis, ou seja, cujos determinantes são não nulos. Este conjunto, formado pelas matrizes quadradas de ordem *n* inversíveis, pode ser denotado por $GL_n(\mathbb{R})$. Para matrizes $A=(a_{ij}),B=(b_{ij})\in GL_n(\mathbb{R})$, o produto entre *A* e *B* é definido como $AB=(c_{ij})$, com $c_{ij}=\sum_{k=1}^{n}a_{ik}b_{kj}$ para todos $1\leq i\leq m$ e $1\leq j\leq n$. Sendo assim, temos o conjunto $GL_n(\mathbb{R})$ sobre o qual está definida a multiplicação de matrizes, operação fechada em $GL_n(\mathbb{R})$. A estrutura $(GL_n(\mathbb{R}),\cdot)$ pode ser classificada como um grupo, sendo as justificativas análogas à do caso anterior. Além disso, esse grupo não é abeliano, o que é evidenciado pelo seguinte exemplo: tomando as matrizes

$$A=\begin{bmatrix}1 & 1 & \cdots & 1\\ 0 & 1 & \cdots & 1\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & 1\end{bmatrix} \quad \text{e} \quad B=\begin{bmatrix}1 & 0 & \cdots & 0\\ 1 & 1 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 1 & 1 & \cdots & 1\end{bmatrix},$$

temos que $AB\neq BA$, porque

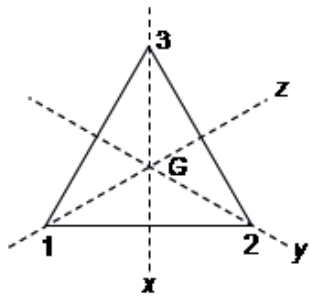
$$AB = \begin{bmatrix} n & n-1 & n-2 & \cdots & 1 \\ n-1 & n-1 & n-2 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 2 & 2 & 2 & \cdots & 1 \\ 1 & 1 & 1 & \cdots & 1 \end{bmatrix} \quad \text{e} \quad BA = \begin{bmatrix} 1 & \cdots & 1 & 1 & 1 \\ 1 & \cdots & 2 & 2 & 2 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 1 & \cdots & n-2 & n-1 & n-1 \\ 1 & \cdots & n-2 & n-1 & n \end{bmatrix}.$$

Portanto, $(GL_n(\mathbb{R}), \cdot)$ é um grupo não abeliano, denominado grupo linear real de grau *n*.

A segunda parte de sua tarefa consiste no estudo dos grupos de simetrias envolvendo figuras geométricas, mais especificamente o grupo de simetria associado aos triângulos equiláteros.

A simetria de um triângulo equilátero T corresponde a qualquer aplicação bijetiva $f: T \to T$ que preserva distâncias. Para analisar o conjunto das simetrias de um triângulo equilátero, representado por S_3, tomemos por base a Figura 2.9, que representa um triângulo equilátero de vértices 1, 2 e 3 com suas medianas x, y e z, sendo a interseção entre essas retas o baricentro G do triângulo.

Figura 2.9 | Triângulo equilátero *T* de vértices 1, 2 e 3 com suas medianas e baricentro



Fonte: elaborada pela autora.

A partir de *T*, conforme a Figura 2.9, podemos estudar as simetrias do triângulo equilátero de modo a compor o conjunto S_3. Podemos indicar por R_0, R_1 e R_2 as rotações segundo ângulos de 0, $\frac{2\pi}{3}$ e $\frac{4\pi}{3}$ radianos em torno de *G*, no sentido anti-horário, e também as reflexões em torno das medianas *x*, *y* e *z* denotadas, respectivamente, por *X*, *Y* e *Z*. Nestes casos, temos as simetrias: $R_0 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$, $R_1 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$, $R_2 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$, $X = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$, $Y = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$ e $Z = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$. Com base no conjunto $S_3 = \{R_0, R_1, R_2, X, Y, Z\}$, podemos definir a composição de transformações, representada por $\circ$. Desta forma, $(S_3, \circ)$ pode ser classificada como um grupo não abeliano, o qual corresponde ao grupo diedral de grau 3.

Logo, para concluir as tarefas referentes ao segundo dia de curso, apresente argumentos que justifiquem porque as estruturas $(GL_n(\mathbb{R}),\cdot)$ e $(S_3,\circ)$ podem ser classificadas como grupos não abelianos, conforme as descrições anteriores e com base nos estudos realizados ao longo da seção. Por fim, organize um texto contemplando as informações referentes aos dois tópicos estudados, elaborando uma apresentação a respeito da importância do conhecimento da teoria de grupos, nesse caso, para o ensino de matrizes e das características dos triângulos equiláteros na Educação Básica.

Avançando na prática

Teoria de grupos e as funções polinomiais

Descrição da situação-problema

Considere que, durante o trabalho com a operação de composição de funções com uma turma do Ensino Médio, você propôs um exercício envolvendo funções polinomiais do 1º grau, isto é, funções $f:\mathbb{R}\to\mathbb{R}$ definidas por $f(x)=ax+b$ em que $a\neq 0$. Em um dos itens deste exercício foram apresentadas as funções $f,g:\mathbb{R}\to\mathbb{R}$, tais que $f(x)=3x$ e $g(x)=4x-1$, sendo exigido dos alunos a identificação das expressões de $(f\circ g)(x)$ e $(g\circ f)(x)$, as quais são dadas por $(f\circ g)(x)=12x-3$ e $(g\circ f)(x)=12x-1$. Durante a resolução deste exercício, um aluno apresentou o seguinte questionamento: "a composição de funções polinomiais de 1º grau sempre resultará em uma função deste mesmo tipo? ". Como você responderia a esta questão? Além disso, considerando o conjunto das funções polinomiais de 1º grau com coeficientes reais, munido da composição de funções, essa estrutura pode ser classificada como um grupo? De que forma podemos justificar a formação de uma estrutura de grupos com base no conjunto e nas operações citados?

Resolução da situação-problema

Leve em conta o conjunto *F* das funções polinomiais de 1º grau com coeficientes reais, considerando $f,g\in F$, tais que $f(x)=ax+b$ e $g(x)=cx+d$, com *a* e *c* não nulos, teremos para todo $x\in\mathbb{R}$ $(f\circ g)(x)=f(g(x))=f(cx+d)=a(cx+d)+b=(acx+ad)+b=(ac)x+(ad+b)$,

em que $ac \neq 0$, logo, $f \circ g \in F$. Sendo assim, F é fechado em relação à composição de funções, o que possibilita concluir que a composição de funções polinomiais de 1º grau com coeficientes reais sempre resultará em uma função deste mesmo tipo, atendendo ao questionamento do aluno.

Em relação à estrutura $(F, \circ)$, além do fechamento, é possível verificar que a propriedade associativa é válida, pois para $f, g, h \in F$ dadas por $f(x) = ax + b$, $g(x) = cx + d$ e $h(x) = px + q$, com a, c e p não nulos, temos $(f \circ g)(x) = (ac)x + (ad + b)$, $(g \circ h)(x) = (cp)x + (cq + d)$ e, assim,

$$((f \circ g) \circ h)(x) = (f \circ g)(px + q) = (ac)(px + q) + (ad + b) = (acp)x + (acq + ad + b)$$

$$(f \circ (g \circ h))(x) = f((cp)x + (cq + d)) = a((cp)x + (cq + d)) + b = (acp)x + (acq + ad + b)$$

para todo $x \in \mathbb{R}$, isto é, $(f \circ g) \circ h = f \circ (g \circ h)$. O elemento neutro da operação considerada é a função identidade, a qual pode ser descrita como: $i : \mathbb{R} \to \mathbb{R}$ tal que $i(x) = x$ para todo $x \in \mathbb{R}$. Por fim, a cada função $f \in F$ com $f(x) = ax + b$, a não nulo, podemos determinar uma função $g \in F$, tal que $g(x) = \frac{1}{a}x - \frac{b}{a}$. Veja que

$$(f \circ g)(x) = f(g(x)) = f\left(\frac{1}{a}x - \frac{b}{a}\right) = a\left(\frac{1}{a}x - \frac{b}{a}\right) + b = x - b + b = x$$

$$(g \circ f)(x) = g(f(x)) = g(ax + b) = \frac{1}{a}(ax + b) - \frac{b}{a} = x + \frac{b}{a} - \frac{b}{a} = x$$

Como $f \circ g = g \circ f = i$, g é a simétrica de f em relação à composição, o que mostra que toda $f \in F$ admite uma função simétrica ou inversa. Como a estrutura $(F, \circ)$ goza das propriedades do fechamento, associativa, existência de elemento neutro e existência de elemento simétrico a todo elemento de F, podemos concluir que $(F, \circ)$ é um grupo. Assim, o conhecimento dos fundamentos teóricos é essencial para que o professor possa verificar, por exemplo, se os questionamentos apresentados pelos alunos procedem, com base nos conceitos e resultados correspondentes, e possa identificar a melhor forma para organizar sua explicação de modo a contribuir com o aprendizado do aluno, considerando seu nível de desenvolvimento atual.

Faça valer a pena

1. Veja os conjuntos descritos a seguir:

$$A = \left\{ x \in \mathbb{R} \,\middle|\, x = \frac{p}{q},\ p, q \in \mathbb{Z}^* \right\}$$

$$B = \{ z \in \mathbb{Z} \mid z = 2k,\ k \in \mathbb{Z} \}$$

$$C = \left\{ \begin{vmatrix} a & b \\ c & d \end{vmatrix} \middle| \; ad - bc \neq 0, \; a,b,c,d \in \mathbb{R} \right\}$$

Em associação com cada conjunto, considere operações de multiplicação usuais correspondentes, as quais podem ser representadas por $\cdot$.
Associe as estruturas $(A,\cdot)$, $(B,\cdot)$ e $(C,\cdot)$ com suas respectivas classificações, conforme as categorias descritas em I, II e III:

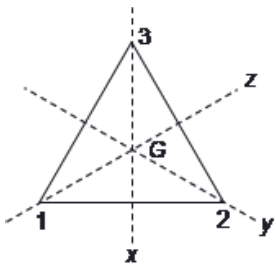
I) Não é um grupo.
II) É um grupo não abeliano.
III) É um grupo abeliano.

Assinale a alternativa que indica todas as associações corretamente:

a) I – $(A,\cdot)$; II – $(C,\cdot)$; III – $(B,\cdot)$.
b) I – $(B,\cdot)$; II – $(C,\cdot)$; III – $(A,\cdot)$.
c) I – $(B,\cdot)$; II – $(A,\cdot)$; III – $(C,\cdot)$.
d) I – $(C,\cdot)$; II – $(A,\cdot)$; III – $(B,\cdot)$.
e) I – $(C,\cdot)$; II – $(B,\cdot)$; III – $(A,\cdot)$.

2. Considere o grupo de simetria do triângulo retângulo representado por $(S_3,\circ)$, no qual o conjunto S_3 é dado por $S_3 = \{R_0, R_1, R_2, X, Y, Z\}$.
Partindo do triângulo equilátero T na forma

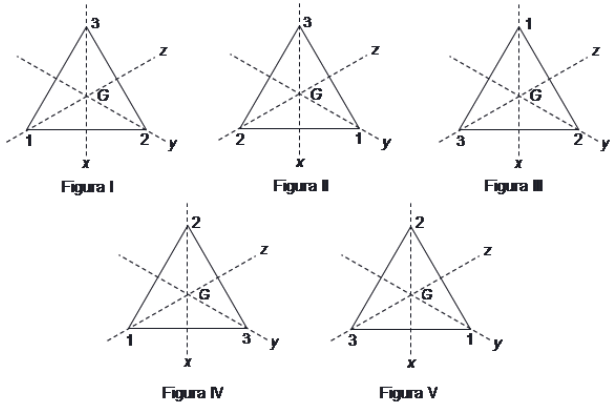
Figura 2.10 | Triângulo equilátero T associado ao grupo $(S_3,\circ)$



Fonte: elaborada pela autora.

deseja-se aplicar a seguinte sequência de transformações sobre T: R_2, Z e R_1, sabendo que o resultado consiste em uma das cinco situações descritas na Figura 2.11.

Figura 2.11 | Simetrias possíveis a partir do triângulo equilátero *T*



Fonte: elaborada pela autora.

Qual dos triângulos indicados na Figura 2.11 descreve o resultado obtido após a aplicação da sequência de transformações indicadas sobre o triângulo *T*?

a) Figura I.
b) Figura II.
c) Figura III.
d) Figura IV.
e) Figura V.

3. Analise as matrizes pertencentes ao conjunto $GL_2(\mathbb{R})$:

$$A=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix};\ B=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix};\ C=\begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix};\ D=\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}$$

A partir dessas matrizes, considere o conjunto $X=\{A, B, C, D\}$ munido da operação usual de multiplicação de matrizes.
Em relação à estrutura $(X,\cdot)$ foram feitas as seguintes afirmações e uma relação proposta entre elas:

I) A estrutura $(X,\cdot)$ pode ser classificada como um grupo finito de ordem 4.

PORQUE

II) A estrutura $(X,\cdot)$ goza da propriedade comutativa.

A respeito das afirmações apresentadas, assinale a alternativa correta:
a) As afirmações I e II estão corretas, e a II é uma justificativa correta para a I.
b) As afirmações I e II estão corretas, mas a II não é uma justificativa correta para a I.
c) A afirmação I está correta e a II incorreta.
d) A afirmação II está correta e a I incorreta.
e) As afirmações I e II estão incorretas.

Seção 2.3

Subgrupos e grupos de permutação

Diálogo aberto

Nas seções anteriores desta unidade estudamos o que são grupos, suas principais propriedades e alguns exemplos importantes, como os derivados dos conjuntos numéricos ou de simetrias. Prosseguindo com nossos estudos, nesta seção analisaremos os subgrupos e os grupos de permutações.

Assim como podemos estabelecer relações entre conjuntos e subconjuntos, podemos comparar grupos a subgrupos, considerando as restrições das operações definidas sobre os subconjuntos. O estudo das restrições é importante quando desejamos avaliar apenas alguns elementos de um conjunto, os quais são selecionados com base em suas características e de acordo com o tema de interesse. Esse tipo de estudo é aplicado, por exemplo, na definição de domínios de funções de uma variável real como subconjuntos de $\mathbb{R}$ para atender às propriedades dos problemas em estudo.

No contexto de estudo desta seção consideremos que para o terceiro dia do curso de formação, os estudos estarão direcionados aos subgrupos. Analisando novamente as tarefas propostas ao longo do curso de formação, no primeiro dia os estudos foram direcionados à definição de grupo e aos grupos numéricos, enquanto no segundo houve uma preocupação com outros conjuntos que também podem ser compor grupos, munidos de operações e propriedades.

Em diversas situações, como na definição do domínio de uma função, por exemplo, precisamos considerar restrições sobre os conjuntos de modo que as operações e as propriedades definidas inicialmente ainda sejam satisfeitas. Assim, no terceiro dia, o objetivo é que os professores de matemática estudem os subgrupos, identificando exemplos que podem ser destacados dentre os grupos estudados nos outros dias de curso, relacionando-os com os conteúdos abordados na Educação Básica. Nesse sentido, sua tarefa está dividida em duas partes, para a primeira, você deve identificar um exemplo de subgrupo a partir dos grupos estudados nos outros dias de curso. A segunda

parte consiste em verificar os problemas propostos em livros do Ensino Médio relacionado ao estudo de funções polinomiais de 1º grau. Após essa análise, você deverá selecionar um problema que, em sua resolução, envolva a definição de uma função real cujo domínio seja um subconjunto do conjunto de números reais sujeito às condições presentes na situação analisada. Além de apresentar o enunciado e sua resolução, você deverá refletir a respeito dos seguintes itens: sendo o domínio da função um subconjunto A do conjunto dos números reais, verifique se A, munido da operação usual de multiplicação definida sobre $\mathbb{R}$, pode ser classificado como subgrupo de $\left(\mathbb{R}^{*},\cdot\right)$. Além disso, para explorar a situação apresentada no problema escolhido, o conjunto A precisa compor um grupo aditivo e um grupo multiplicativo, munido, respectivamente, das operações usuais de adição e multiplicação de números reais? Como você justificaria essas informações?

Que grupos podem ser estudados a partir desses questionamentos? Qual é a importância do conceito de subgrupo para o estudo das questões propostas? Como o conceito de subgrupo pode contribuir com a formação do professor de Matemática da Educação Básica?

Com esses conhecimentos, você estará apto a finalizar o curso e a elaborar um documento que sintetize todas as reflexões realizadas e outros questionamentos que possam surgir ao longo do curso. Assim, finalize as tarefas propostas elaborando um texto que deve conter o problema selecionado no terceiro dia de curso, as análises realizadas com base no problema escolhido, destacando a fundamentação teórica para cada tema. Não se esqueça de incluir também as tarefas que foram desenvolvidas nos outros dois dias de curso, apresentando, ao final do documento, uma conclusão a respeito da importância desse tipo de capacitação para a formação do professor de Matemática da Educação Básica bem como a importância da teoria de grupos nesse contexto.

Não pode faltar

Nas seções anteriores, estudamos que um grupo $(A,*)$ corresponde a uma estrutura algébrica definida a partir de um conjunto não vazio A, munido de uma operação binária $*$, na qual são desfrutadas as propriedades do fechamento, associativa, existência de elemento neutro e existência de elemento simetrizável a todo elemento de A. Porém, em alguns casos, ao invés de analisar

todos os elementos de A, desejamos investigar apenas um de seus subconjuntos, considerando a mesma operação $*$, como no caso em que desejamos restringir o domínio de uma função a um de seus subconjuntos. Para isso, é importante estudarmos os subgrupos.

Subgrupos

Considere um grupo $(A,*)$ e um subconjunto $B \subset A$ não vazio. Dizemos que $(B,*)$ é um **subgrupo** de $(A,*)$ se as seguintes condições forem verificadas:

- B é fechado para a operação $*$, isto é, se $x,y \in B$ então $x*y \in B$.
- $(B,*)$, em particular, pode ser classificado como um grupo, considerando que $*$, neste caso, denota a restrição da operação $*$ ao conjunto B.

A partir da definição, temos as seguintes **observações**:

- A propriedade associativa sempre é válida na estrutura $(B,*)$: como os elementos de B, em particular, são elementos de A, e a associatividade é válida a todos os elementos de A, então podemos concluir que a expressão $a*(b*c)=(a*b)*c$ é verdadeira para todos $a,b,c \in B \subset A$.
- O elemento neutro e_B de $(B,*)$ é igual ao elemento neutro e de $(A,*)$. Com efeito, se $a \in B \subset A$, então $a*e_B = a = a*e$, porque o elemento e_B assim como e são neutros. Aplicando o elemento $a^{-1} \in B \subset A$, o qual existe porque $(B,*)$ é grupo, à esquerda da última expressão obtemos $a^{-1}*(a*e_B)=a^{-1}*(a*e)$, isto é, $e_B = e$.
- A cada $x \in B$, o simétrico no conjunto B é igual ao simétrico em A. De fato, se x^{-1} é o simétrico de x em B, é válido que $x^{-1}*x = x*x^{-1} = e_B$, mas como $e_B = e$, temos $x^{-1}*x = x*x^{-1} = e$, o que implica que x^{-1} é o simétrico de x em A.

Assimile

Se $e \in A$ corresponde ao elemento neutro relativo à operação $*$, então o conjunto $\{e\}$, munido da operação $*$, pode ser classificado como um subgrupo de $(A,*)$. Além disso, como A é um subconjunto de si mesmo, então $(A,*)$ é um subgrupo de $(A,*)$. Estes dois subgrupos, $(\{e\},*)$ e $(A,*)$ são denominados **subgrupos triviais** de $(A,*)$.

Reflita

Por que $(\{e\},*)$ corresponde a um subgrupo de $(A,*)$, sendo $e \in A$ o elemento neutro do grupo $(A,*)$? Como podemos justificar esse fato?

Por exemplo, considere o grupo aditivo dos reais, $(\mathbb{R},+)$. Sabemos que $\mathbb{Z} \subset \mathbb{R}$, pois todo número inteiro é também real. Além disso, quando restringimos a operação de adição definida sobre $\mathbb{R}$ ao conjunto $\mathbb{Z}$, podemos observar que:

- $\mathbb{Z}$ é fechado para a adição de reais, porque a soma de números inteiros é também um inteiro, ou seja, se $x, y \in \mathbb{Z}$, então $x + y \in \mathbb{Z}$.
- $(\mathbb{Z},+)$ pode ser classificado como um grupo, pois com a restrição da adição de reais aos inteiros, além do fechamento, são válidas as propriedades associativa, existência de elemento neutro (o qual corresponde ao $0 \in \mathbb{Z}$) e a existência de elemento simetrizável a todo inteiro (se $x \in \mathbb{Z}$ então seu simétrico será $-x \in \mathbb{Z}$).

Logo, $(\mathbb{Z},+)$ corresponde a um subgrupo de $(\mathbb{R},+)$. Lembre-se que o grupo aditivo dos inteiros $(\mathbb{Z},+)$ já foi estudado na Seção 2.1.

Uma situação análoga pode ser observada quando consideramos $\mathbb{Q} \subset \mathbb{R}$, pois $(\mathbb{Q},+)$ é um subgrupo de $(\mathbb{R},+)$. Analise as justificativas para este caso com base na definição de subgrupo.

Além da definição, podemos empregar uma proposição para caracterizar os subgrupos:

Proposição 1: Sejam $(A,*)$ um grupo e B um subconjunto não vazio de A. Então $(B,*)$ é um subgrupo de $(A,*)$ se, e somente se, as seguintes condições forem satisfeitas:

(i) Para todos $x, y \in B$ for válido que $x * y \in B$.

(ii) Para todo $x \in B$ tivermos que $x^{-1} \in B$.

Demonstração: Supondo que $(B,*)$ é um subgrupo de $(A,*)$ temos que a condição (i) é válida, porque refere-se à propriedade do fechamento, a qual é satisfeita em $(B,*)$. Se $x \in B$, por $(B,*)$ ser um grupo, existe $x^{-1} \in B$ que satisfaz à condição $x^{-1} * x = x * x^{-1} = e_B$, e como o elemento simétrico é o mesmo nas estruturas $(A,*)$ e $(B,*)$, então o simétrico x^{-1} em A é também elemento de B. Reciprocamente,

suponha que as condições (i) e (ii) são válidas, o que implica na validade do fechamento em $(B,*)$, consequência da condição (i). Verificamos anteriormente que a associatividade é válida em $(B,*)$ em decorrência da associatividade em $(A,*)$. Para a existência de elemento neutro note que, ao tomar $x \in B$, segue da condição (ii) que existe $x^{-1} \in B$ e assim, como o fechamento é válido, $e = x^{-1} * x \in B$. A existência de elemento simetrizável é válida em B como consequência da condição (ii). Portanto, $(B,*)$ é um subgrupo de $(A,*)$, o que conclui a demonstração.

Assimile

Para verificar que uma estrutura $(B,*)$ é subgrupo de $(A,*)$, com $B \subset A$ não vazio, podemos empregar a definição, justificando todas as propriedades necessárias, ou utilizar as implicações presentes na proposição 1, comprovando a validade das condições: para todos $x,y \in B$ é válido que $x * y \in B$ e que $x^{-1} \in B$.

Exemplificando

Considere o grupo multiplicativo $(\mathbb{R}^*,\cdot)$. Vamos verificar que a estrutura $(K,\cdot)$, com $K = \{x \in \mathbb{R}^* \mid x > 0\}$, é um subgrupo de $(\mathbb{R}^*,\cdot)$ empregando a proposição 1.

Veja que se $a,b \in K$, então a e b são números positivos. Logo, o produto entre a e b será também um número positivo, isto é, $ab > 0$. Sendo assim, $ab \in K$, o que comprova a validade da condição (i).

Além disso, se $x \in K$, $x > 0$, então no grupo $(\mathbb{R}^*,\cdot)$ teremos que o simétrico existe e é tal que $x^{-1} > 0$, ou seja, $x^{-1} \in K$, validando a igualdade $x^{-1} \cdot x = x \cdot x^{-1} = 1$. Como K contém o simétrico associado a todo elemento $x \in K$, podemos concluir que a condição (ii) é válida.

Das condições (i) e (ii) podemos concluir, em conjunto com a proposição 1, que $(K,\cdot)$ é um subgrupo de $(\mathbb{R}^*,\cdot)$.

Podemos ainda destacar outros exemplos de subgrupos, tais como:

- $(2\mathbb{Z},+)$ com $2\mathbb{Z} = \{...,-4,-2,\ 0,\ 2,\ 4,...\}$ pode ser classificado como subgrupo de $(\mathbb{Z},+)$.
- $(3\mathbb{Z},+)$ com $3\mathbb{Z} = \{...,-6,-3,\ 0,\ 3,\ 6,...\}$ pode ser classificado como subgrupo de $(\mathbb{Z},+)$.

- Sendo $\mathbb{Q} \subset \mathbb{R}$, $(\mathbb{Q}^*, \cdot)$ corresponde a um subgrupo de $(\mathbb{R}^*, \cdot)$.
- $(M_3(\mathbb{R}), +)$, composto pelas matrizes quadradas de ordem 3 com entradas reais, pode ser classificado como um subgrupo de $(M_{m \times n}(\mathbb{R}), +)$.
- $(R, \circ)$, em que $R = \{R_0, R_1, R_2\}$ contém as rotações do triângulo equilátero, é um subgrupo de $(S_3, \circ)$.

Analise estes exemplos e, como sugestão de estudo, verifique como podemos justificar que cada estrutura pode ser classificada como subgrupo dos grupos correspondentes, baseando-se definição ou na proposição apresentada.

Exemplificando

Considere o grupo $(\mathbb{R}^*, \cdot)$. Note que $\mathbb{Z}^* \subset \mathbb{R}^*$ e a partir dele podemos compor a estrutura $(\mathbb{Z}^*, \cdot)$. Quando restringimos a operação de multiplicação aos inteiros não nulos, observamos que nem todo elemento desse conjunto admite um simétrico em relação a multiplicação, pois os únicos elementos que satisfazem a essas propriedades são os números -1 e 1, os quais são inversos deles próprios. Assim, apesar de ser válida a inclusão $\mathbb{Z}^* \subset \mathbb{R}^*$, a restrição da multiplicação aos inteiros não nulos não satisfaz a propriedade de existência de elemento simétrico a todo elemento do conjunto. Logo, $(\mathbb{Z}^*, \cdot)$ não é subgrupo de $(\mathbb{R}^*, \cdot)$, visto que $(\mathbb{Z}^*, \cdot)$, em particular, não pode ser classificado como subgrupo. Dessa forma, nem todo subconjunto originado de um grupo pode ser classificado como subgrupo.

Na seção anterior estudamos um tipo especial de grupo relacionado à Geometria, os grupos de simetrias. Além deste, existe um outro caso importante de grupo, que são denominados grupos de permutações.

Grupos de permutações

Permutação é um termo que designa, na teoria dos grupos, as funções bijetivas cujo domínio e contradomínio correspondem a um mesmo conjunto.

Considere a situação de um sorteio de números em um jogo da loteria, por exemplo. Suponha que em determinado jogo foram

sorteados os números 2, 16, 35 e 11, nesta ordem. Observe que estes mesmos números poderiam ter sido sorteados na sequência 11, 16, 2 e 35, por exemplo, ou ainda, poderíamos organizá-los em ordem crescente como 2, 11, 16 e 35, sendo que em cada uma dessas possibilidades todos os elementos são considerados. Note que a partir de um mesmo conjunto, $C = \{2, 11, 16, 35\}$, os elementos podem ser representados a partir de diferentes ordens, cada uma dessas representações é denominada permutação dos elementos do conjunto C. Podemos ainda, com base nessa situação, construir um conjunto que contenha todas as possíveis permutações dos elementos de C.

Com base em situações que apresentam características semelhantes a essas e no conceito de permutação, vamos estudar os grupos que podem ser construídos com base nas permutações.

Se A corresponde a um conjunto não vazio, podemos denotar por $S(A)$ o conjunto formado por todas as permutações que podem ser construídas com base nos elementos de A, dessa forma, os elementos de $S(A)$ são bijeções na forma $f : A \to A$. Sobre o conjunto $S(A)$ podemos definir a operação de composição de aplicações, de tal modo que se $f, g \in S(A)$ então $f : A \to A$ e $g : A \to A$, o que possibilita a construção da composição $g \circ f : A \to A$, a qual também é um elemento de $S(A)$ por se tratar de uma bijeção sobre A. Devido a esse fato, na estrutura $(S(A), \circ)$ é válida a propriedade do fechamento.

Reflita

Por que a composição $g \circ f : A \to A$ das bijeções $f : A \to A$ e $g : A \to A$ pode ser classificada como uma bijeção?

A composição de aplicações é associativa em $(S(A), \circ)$. De fato, se $f, g, h \in S(A)$, então $((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x)))$ e $(f \circ (g \circ h))(x) = f(g \circ h(x)) = f(g(h(x)))$, para todo $x \in A$, o que implica em $(f \circ g) \circ h = f \circ (g \circ h)$ para todos $f, g, h \in S(A)$.

A estrutura $(S(A), \circ)$ admite como elemento neutro a aplicação $i_A : A \to A$ dada por $i_A(x) = x$ para todo $x \in A$, ou seja, o elemento neutro corresponde à aplicação idêntica de A. Esta aplicação é bijetiva e satisfaz a condição de ser elemento neutro, pois se $f \in S(A)$, para todo $x \in A$ é válido que $(f \circ i_A)(x) = f(i_A(x)) = f(x)$ e $(i_A \circ f)(x) = i_A(f(x)) = f(x)$, sendo assim, $f \circ i_A = i_A \circ f = f$ para todo $f \in S(A)$.

Como qualquer aplicação $f \in S(A)$ é uma bijeção, então f admite uma inversa $f^{-1}: A \to A$, a qual corresponde a uma bijeção e, assim, $f^{-1} \in S(A)$. Por se tratar de uma aplicação inversa, a expressão $f \circ f^{-1} = f^{-1} \circ f = i_A$ será válida. Logo, $f^{-1} \in S(A)$ corresponde ao elemento simétrico de $f \in S(A)$.

Como a estrutura $(S(A), \circ)$ goza das propriedades do fechamento, associativa, existência de elemento neutro e de elemento simétrico a todo elemento de $S(A)$, podemos concluir que $(S(A), \circ)$ é um grupo denominado **grupo de permutações** sobre A.

Faça você mesmo

Mostre que o grupo de permutações $(S(A), \circ)$ será classificado como grupo abeliano somente se o conjunto $S(A)$ contiver um, ou no máximo, dois elementos.

Exemplificando

Considere o conjunto $E = \{1, 2, 3\}$. Vamos identificar todas as permutações envolvendo os elementos do conjunto E.

A primeira permutação é a idêntica, em que os elementos de E não sofrem alterações em suas posições e pode ser denotada como

$$f_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

As outras permutações possíveis podem ser descritas como segue:

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

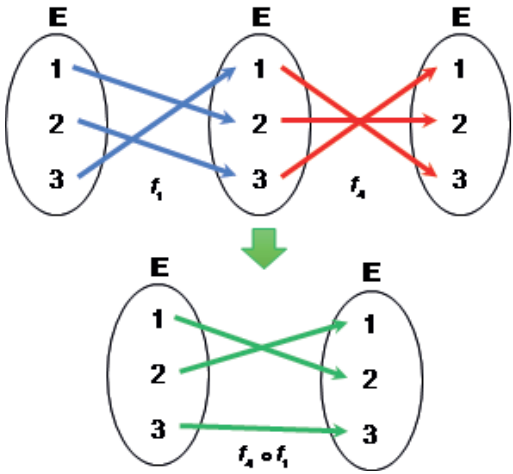
$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \text{ e } f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Podemos, assim, construir o conjunto $S(E) = \{f_0, f_1, f_2, f_3, f_4, f_5\}$ composto por todas as bijeções envolvendo os elementos de E.

Definindo a operação de composição de aplicações sobre o conjunto $S(E)$ podemos compor a estrutura $(S(E), \circ)$, a qual já verificamos que é um grupo.

Por exemplo, podemos identificar a composição $f_4 \circ f_1$ por meio da representação em diagramas, conforme a Figura 2.12.

Figura 2.12 | Composição $f_4 \circ f_1$ na estrutura $(S(E), \circ)$



Fonte: elaborada pela autora.

Ou ainda,

$$f_4 \circ f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = f_5$$

Podemos construir todas as combinações entre elementos de $S(E)$ com base na composição de aplicações, o que possibilita a construção da tábua de operação indicada na Figura 2.13.

Figura 2.13 | Tábua associada ao grupo $(S(E), \circ)$

$\circ$	f_0	f_1	f_2	f_3	f_4	f_5
f_0	f_0	f_1	f_2	f_3	f_4	f_5
f_1	f_1	f_2	f_0	f_5	f_3	f_4
f_2	f_2	f_0	f_1	f_4	f_5	f_3
f_3	f_3	f_4	f_5	f_0	f_1	f_2
f_4	f_4	f_5	f_3	f_2	f_0	f_1
f_5	f_5	f_3	f_4	f_1	f_2	f_0

Fonte: elaborada pela autora.

Podemos construir um subgrupo a partir de $(S(E),\circ)$. Tomando o conjunto $P=\{f_0, f_1, f_2\}$, com a operação de composição restrita a ele, a estrutura $(P,\circ)$ corresponde a um subgrupo de $(S(E),\circ)$.

Como complementação aos estudos, verifique que $(P,\circ)$ satisfaz a todas as propriedades da definição de subgrupo, construindo a tábua correspondente. Note que as relações entre os elementos de *P* pela composição podem ser obtidas a partir da tábua de $(S(E),\circ)$.

Agora, podemos generalizar a situação descrita no exemplo anterior para um conjunto qualquer na forma $A=\{1, 2, ..., n\}$, com $n \geq 1$.

Os grupos de permutações, que são construídos com base nos conjuntos na forma $A=\{1, 2, ..., n\}$ com $n \geq 1$, são chamados de **grupos simétricos de grau *n*** e são denotados como $(S_n,\circ)$. Pela análise combinatória, como *A* contém *n* elementos, então podemos construir uma quantidade de permutações igual a $n!$, assim, $(S_n,\circ)$ corresponde a um grupo finito com uma quantidade $n!$ de elementos, ou seja, um grupo finito de ordem $n!$.

Faça você mesmo

Estude o grupo simétrico de grau 2, $(S_2,\circ)$ e construa a tábua de operação correspondente.

Pesquise mais

Para complementar os estudos a respeito da teoria de grupos, com seus principais exemplos, e o conceito de subgrupo, consulte os capítulos 2 e 3 da dissertação a seguir.

SOUZA, Rodrigo Luiz. **Uma breve introdução à teoria de grupos**. 2014, 73 f. Dissertação (Mestrado) – Centro de Ciências Físicas e Matemáticas, Universidade Federal de Santa Catarina, Florianópolis. 2014. Disponível em: <https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/123275/326843.pdf?sequence=1&isAllowed=y>. Acesso em: 16 jul. 2018.

Sem medo de errar

No último dia do curso de formação continuada o tema de estudo são os subgrupos e suas propriedades. Sua tarefa, neste dia, está dividida em partes e relacionada às tarefas cumpridas nos outros dias de curso. Inicialmente, você deve identificar exemplos de subgrupos a partir dos grupos já estudados no curso.

Dentre os grupos estudados nos dois primeiros dias de curso, podemos destacar o grupo linear de grau *n* composto pelas matrizes quadradas inversíveis de ordem *n*, representado por $(GL_n(\mathbb{R}),\cdot)$, o qual corresponde a um grupo multiplicativo construído a partir do conjunto de matrizes. A partir desse grupo podemos construir a estrutura $(GL_2(\mathbb{R}),\cdot)$, composta pelas matrizes quadradas de ordem 2 inversíveis, a qual corresponde a um subgrupo de $(GL_n(\mathbb{R}),\cdot)$.

Provemos que $(GL_2(\mathbb{R}),\cdot)$ corresponde a um subgrupo de $(GL_n(\mathbb{R}),\cdot)$ pela proposição 1. Se $A=(a_{ij})$ e $B=(b_{ij})$ são elementos de $GL_2(\mathbb{R})$, então suas entradas são números reais que satisfazem $\det(A)=a_{11}a_{22}-a_{12}a_{21}\neq 0$ e $\det(B)=b_{11}b_{22}-b_{12}b_{21}\neq 0$. Note que

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

Como as entradas de *AB* são combinações entre números reais pela soma e multiplicação, então todas as suas entradas são números reais. Além disso, pelas propriedades de determinante de matrizes, temos que $\det(AB)=\det(A)\det(B)\neq 0$, porque ambos determinantes de *A* e *B* são não nulos. Logo, a propriedade do fechamento é satisfeita para $(GL_2(\mathbb{R}),\cdot)$. Além disso, tomando $A=(a_{ij})\in GL_2(\mathbb{R})$, temos que *A* admite inversa A^{-1}, a qual assume a forma $A^{-1}=\frac{1}{\det(A)}\begin{pmatrix}a_{22} & -a_{12}\\ -a_{21} & a_{11}\end{pmatrix}$, cujas entradas são todos números reais, admitindo, pelas propriedades dos determinantes, $\det(A^{-1})=\frac{1}{\det(A)}$, isto é, $A^{-1}\in GL_2(\mathbb{R})$. Logo, como as condições (i) e (ii) da proposição 1 são satisfeitas, podemos concluir que $(GL_2(\mathbb{R}),\cdot)$ é um subgrupo de $(GL_n(\mathbb{R}),\cdot)$.

Na segunda parte do curso, você deve selecionar um problema do Ensino Médio que permita o estudo de funções polinomiais de 1º grau e que envolva a definição de funções cujos domínios sejam restrições a subconjuntos de $\mathbb{R}$.

Um tipo de problema que pode ser abordado no estudo das funções polinomiais de 1º grau é o seguinte:

Um taxista cobra de seus passageiros uma taxa fixa de R$ 4,00 além R$ 3,00 por quilômetro rodado, sendo a tarifa contabilizada apenas quilometragens positivas. Com base nessas informações, qual função representa a situação descrita? Qual deve ser a quilometragem percorrida pelo taxista para que a tarifa cobrada seja de R$ 79,00?

No caso desse problema, como a tarifa é dada em função da quilometragem, podemos expressar essa relação por meio de uma função em que a variável independente é a quilometragem e a dependente é a tarifa. Admitindo *q* como a quilometragem percorrida e *t* a tarifa cobrada, a expressão que relaciona essas variáveis é dada por $t(q) = 4 + 3q$.

As quilometragens são avaliadas a partir do conjunto de números racionais não nulos, pois devemos considerar quilometragens positivas conforme as informações do enunciado. Além disso, adotamos o conjunto dos racionais porque, em geral, os instrumentos de medições nos informam apenas distâncias com uma quantidade limitada de casas decimais. Devido a essas informações, o domínio da função que descreve o problema apresentado deve ser dado pelo conjunto $\mathbb{Q}_+^*$.

Note que $(\mathbb{Q}_+^*, \cdot)$ é um subgrupo de $(\mathbb{R}^*, \cdot)$. De fato, a multiplicação goza da propriedade do fechamento em $\mathbb{Q}_+^*$, porque o produto entre números racionais positivos resulta em um racional positivo. Além disso, se $x \in \mathbb{Q}_+^*$, seu inverso existe e é tal que $\frac{1}{x} \in \mathbb{Q}_+^*$, satisfazendo a igualdade $x \cdot \frac{1}{x} = \frac{1}{x} \cdot x = 1$, com 1 sendo o elemento neutro da estrutura considerada. Logo, pela proposição 1, temos que é válida a relação de subgrupo entre $(\mathbb{Q}_+^*, \cdot)$ e $(\mathbb{R}^*, \cdot)$.

Além disso, considerando a expressão construída, devemos determinar a quilometragem *q* para que a tarifa seja de R$ 79,00, ou seja, resolver a equação $79 = 4 + 3q$. Assim como discutido no primeiro dia de curso, as propriedades necessárias para a resolução desta equação são: existência de elemento simétrico, associatividade e existência de elemento neutro para a adição e para a multiplicação. Por isso, para a resolução desta parte do problema, o conjunto $\mathbb{Q}_+^*$, domínio da função, deve compor um grupo aditivo e multiplicativo para as operações usuais, fato este que pode ser verificado. Temos que $(\mathbb{Q}_+^*, +)$ não é um grupo aditivo porque não contém o elemento neutro 0 da adição, o que inviabiliza a resolução de parte deste problema. Assim, para que possamos concluir este

problema, precisaríamos da estrutura $(\mathbb{Q}_+^*, \cdot)$ e da estrutura $(\mathbb{Q}_+, +)$, as quais podem ser classificadas como grupos.

Qual é a importância do conceito de subgrupo para o estudo do problema selecionado? Como você observa a aplicabilidade dos conhecimentos da teoria de grupos para o trabalho com a álgebra na Educação Básica?

Com esses conhecimentos, você estará apto a finalizar o curso de formação e redigir o relatório final. Conclua as tarefas propostas nesta seção por meio da elaboração de um texto contemplando as resoluções para todas as tarefas propostas nos três dias de curso, incluindo as reflexões realizadas durante os estudos, finalizando com uma conclusão que evidencie a importância da teoria de grupos para a formação de professor, bem como as contribuições da formação continuada para trabalho pedagógico.

Avançando na prática

Associação entre grupos de permutações e de simetrias

Descrição da situação-problema

Suponha que você deseja propor uma tarefa para uma turma de Ensino Médio com vistas a associar os campos da Geometria e da Análise Combinatória. Nesse sentido, você pretende elaborar uma proposta que envolva o estudo das propriedades dos triângulos equilátero e suas simetrias, tópico da Geometria Plana, com o conceito de permutação, próprio da Análise Combinatória. Do ponto de vista da teoria de grupos, como podemos associar os temas simetrias dos triângulos equiláteros e permutações? Em geral, como podemos relacionar os grupos de permutações e os grupos de simetrias? Analise as questões propostas e conclua o estudo elaborando uma tarefa para o Ensino Médio que aborde a relação entre as simetrias dos triângulos equiláteros com o conceito de permutação.

Resolução da situação-problema

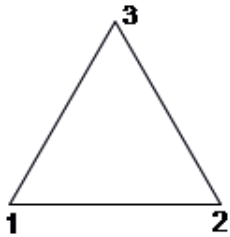
Para analisar as questões propostas, considere o grupo das simetrias do triângulo retângulo $(S_3, \circ)$ munido com a composição de

aplicações. Tomando por base o triângulo equilátero T apresentado na Figura 2.14, o conjunto $S_3 = \{R_0, R_1, R_2, X, Y, Z\}$ é tal que

$$R_0 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \quad R_1 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}, \quad R_2 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix},$$

$$X = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \quad Y = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \text{ e } Z = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$$

Figura 2.14 | Triângulo equilátero T de vértices 1, 2 e 3



Fonte: elaborada pela autora.

Note que os elementos de S_3 indicam as possíveis transformações que podem ser aplicadas sobre o triângulo equilátero T de modo a mantê-lo com um mesmo formato, mas alterando o posicionamento de seus vértices. Podemos interpretar cada uma dessas transformações como uma permutação aplicada sobre os vértices de T e, dessa forma, associar o grupo $(S_3, \circ)$ com o grupo de permutações envolvendo três elementos, $(S(E), \circ)$ em que $E = \{1, 2, 3\}$. Assim, os grupos simétricos de grau 3 podem ser associados ao grupo de simetrias do triângulo equilátero.

Note que, no caso de $(S(E), \circ)$, o conjunto $S(E) = \{f_0, f_1, f_2, f_3, f_4, f_5\}$ é tal que

$$f_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Comparando $(S_3, \circ)$ e $(S(E), \circ)$, munidos com a composição de transformações, é possível observar que $f_0 \equiv R_0$, $f_1 \equiv R_2$, $f_2 \equiv R_1$, $f_3 \equiv Z$, $f_4 \equiv Y$ e $f_5 \equiv X$. Assim, podemos notar que o grupo $(S(E), \circ)$ pode ser interpretado, geometricamente, como o grupo das simetrias de um triângulo equilátero de vértices 1, 2 e 3, tornando-o equivalente ao grupo das simetrias $(S_3, \circ)$.

Dessa forma, de modo geral, quando temos um grupo de simetria $(S_n, \circ)$, $n \geq 1$, podemos associá-lo a um grupo simétrico de grau n $(S(A), \circ)$, com $A = \{1, 2, ..., n\}$, $n \geq 1$.

Como abordar essa associação a partir dos conteúdos vistos na Educação Básica? Assim, para finalizar esses estudos, elabore uma proposta voltada a uma turma do Ensino Médio que possibilite a associação entre as simetrias dos triângulos equiláteros com o conceito de permutação, abordado no estudo da Análise Combinatória.

Faça valer a pena

1. Podemos justificar que determinadas estruturas são subgrupos de certos grupos com base na definição ou em proposições equivalentes. Com isso, considere o grupo aditivo $(\mathbb{Z}, +)$. Com base nessa estrutura, analise as seguintes afirmações, classificando-as como verdadeiras (V) ou falsas (F):

( ) A estrutura <<Eqn283.eps>>, em que $4\mathbb{Z} = \{z \in \mathbb{Z} \mid z = 4k \text{ para algum } k \in \mathbb{Z}\}$, pode ser classificada como subgrupo de $(\mathbb{Z}, +)$.
( ) A estrutura $(K, +)$, em que $K = \{z \in \mathbb{Z} \mid z = 2k + 1 \text{ para algum } k \in \mathbb{Z}\}$, pode ser classificada como subgrupo de $(\mathbb{Z}, +)$.
( ) A estrutura $(D, +)$, em que $D = \{-1, 1\}$, pode ser classificada como subgrupo de $(\mathbb{Z}, +)$.

Assinale a alternativa que indica todas as classificações corretamente, na ordem em que as afirmações foram apresentadas:

a) V – F – V.
b) V – V – F.
c) V – F – F.
d) F – V – F.
e) F – F – V.

2. Seja um grupo $A = \{1, 2, 3\}$, a partir do qual é construído o grupo de simetrias de grau 3 representado por $(S(A), \circ)$, isto é, o grupo composto por todas as permutações dos elementos de A, munido da operação de composição de transformações. O conjunto $S(A) = \{f_0, f_1, f_2, f_3, f_4, f_5\}$ é tal que

$$f_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Com base no grupo descrito, seja a seguinte igualdade:

$$\left(\left(f_1 \circ f_4\right) \circ X\right) \circ f_3 = f_4$$

Considerando as informações apresentadas, assinale a alternativa que indica qual deve ser o elemento $X \in S(A)$ para que a igualdade anterior seja verdadeira:

a) $X = f_2$.
b) $X = f_4$.
c) $X = f_3$.
d) $X = f_1$.
e) $X = f_5$.

3. Considere o conjunto $T = \{0, 1, 2, 3, 4, 5\} \subset \mathbb{Z}$ sobre o qual está definida a operação $\oplus$ descrita como $x \oplus y$ corresponde ao resto da divisão, em $\mathbb{Z}$, de $x + y$ por 6, em que $x, y \in T$.
Com base na estrutura $(T, \oplus)$, foram propostas as seguintes afirmações e uma relação entre elas:

I. A estrutura $(R, \oplus)$, com $R = \{0, 3\}$, pode ser classificada como um subgrupo do grupo $(T, \oplus)$.

PORQUE

II. Na estrutura $(R, \oplus)$ é válida a propriedade comutativa.

Em relação às informações apresentadas, assinale a alternativa correta.

a) As afirmações I e II estão corretas, e a II é uma justificativa correta para a I.
b) As afirmações I e II estão corretas, mas a II não é uma justificativa correta para a I.
c) A afirmação I está correta e a II incorreta.
d) A afirmação II está correta e a I incorreta.
e) As afirmações I e II estão incorretas.

Referências

COCHMANSKI, Julio Cesar; COCHMANSKI, Liliane Cristina de Camargo. **Estruturas algébricas**. Curitiba: InterSaberes, 2016.

DOMINGUES, Hygino H.; IEZZI, Gelson. **Álgebra moderna**. São Paulo: Atual, 2003.

GARCIA, Arnaldo; LEQUAIN, Yves. **Elementos de álgebra**. Rio de janeiro: IMPA, 2015.

HEFEZ, Abramo. **Curso de álgebra**. v. 1. Rio de Janeiro: IMPA, 2014.

LEITE, Álvaro Emílio; CASTANHEIRA, Nelson Pereira. **Teoria dos números e teoria dos conjuntos**. Curitiba: InterSaberes, 2014.

MACHADO, Milca Pires. Que Matemática está por trás do cubo mágico? **Mostra interativa da produção estudantil em educação científica e tecnológica**, 2017. Disponível em: <https://www.publicacoeseventos.unijui.edu.br/index.php/moeducitec/article/view/8524/7315>. Acesso em: 16 jul. 2018.

REIS, Elisandra Regina Sampaio dos. **Estudo de simetria e seu ensino no nível fundamental e médio**. 2013, 58 f. Dissertação (Mestrado Profissional em Matemática) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Paulo.

SANTOS, José Plínio de Oliveira. **Introdução à teoria dos números**. Rio de Janeiro: IMPA, 2015.

SANTOS, Josiane Oliveira dos. **Álgebra no cubo Rubik**. 2010. Monografia (Licenciatura em Matemática) – Universidade Federal do Amapá, Macapá, 2010.

SOUZA, Rodrigo Luiz de. **Uma Breve Introdução à Teoria de grupos**. 2014. Dissertação (Mestrado) – Centro de Ciências Físicas e Matemáticas, Universidade Federal de Santa Catarina, Florianópolis, 2014. Disponível em: <https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/123275/326843.pdf?sequence=1&isAllowed=y>. Acesso em: 16 jul. 2018.

VIEIRA, Ana Cristina. **Fundamentos de álgebra I**. Belo Horizonte: Editora UFMG, 2011.

Estruturas algébricas: anéis

Convite ao estudo

Na Unidade 1 discutimos a respeito de tópicos da Teoria dos Números e Teoria de Conjuntos, observando a sua aplicabilidade na definição de grupo, estrutura estudada na Unidade 2, e que possui aplicação na resolução de problemas matemáticos devido às propriedades associadas. Nesta unidade estudaremos outra estrutura algébrica importante: o anel. Este conceito está presente na estruturação, por exemplo, dos conjuntos numéricos, de matrizes e de funções. A classificação de conjuntos e operações como anéis possibilita o emprego de diversas propriedades, como a distributividade, a associatividade, entre outros, na resolução de problemas modelados matematicamente.

Tendo em vista a investigação desse conceito essencial da álgebra, para essa unidade, suponha que você seja funcionário de uma empresa do ramo de tecnologia. Sua função, em conjunto com uma equipe de funcionários, consiste em dar suporte ao setor de programação, auxiliando-os na estruturação dos algoritmos responsáveis pelo funcionamento de certos equipamentos. O funcionamento das máquinas produzidas pelas indústrias atendidas por essa empresa é possível devido ao emprego de conceitos da álgebra na construção dos algoritmos computacionais.

Devido ao crescimento no número de indústrias atendidas, você foi designado pela empresa para capacitar uma equipe de funcionários que irá auxiliá-lo na análise dos algoritmos elaborados pelo setor de programação. Assim, você deverá construir uma capacitação com foco no estudo dos anéis e suas principais

propriedades, porque este é um dos conceitos essenciais que fundamentam os algoritmos elaborados pela empresa.

Este curso de capacitação deverá ser desenvolvido em três etapas, e você precisa entregar os materiais ao gerente do setor de programação a fim de que os preparativos para a capacitação sejam feitos. Assim, você deverá entregar o plano do treinamento, o qual deve conter os problemas que serão propostos aos funcionários, as possíveis soluções e comentários a respeito dos conteúdos que devem ser desenvolvidos para a execução de cada tarefa proposta.

Na primeira etapa, o tema é o estudo das propriedades dos conjuntos numéricos e a possibilidade de associação com a definição de anel, a segunda etapa será voltada ao estudo do conjunto de matrizes e a associação deste com as categorias de anéis, por fim, na última etapa serão estudados os anéis dos inteiros módulo m, relacionando esta estrutura com a propriedade da integridade.

Dessa forma, para cumprir esse desafio, estudaremos na Seção 3.1 a definição de anel e algumas propriedades importantes, além dos anéis numéricos. Na Seção 3.2 estudaremos os anéis com unidade e anéis comutativos, bem como os subanéis. Por fim, na Seção 3.3 estudaremos os domínios de integridade e as relações existentes entre as subcategorias de anéis.

Quais conhecimentos matemáticos precisam ser estudados pelos funcionários para que eles possam atuar no ramo da avaliação de algoritmos? Quais são os principais conjuntos que podem ser empregados na construção dos algoritmos computacionais? Dê continuidade aos seus estudos e analise a primeira tarefa que deve ser cumprida.

Seção 3.1

Estruturas algébricas: estudo dos anéis

Diálogo aberto

Nesta primeira seção discutiremos o conceito de anel. Na unidade anterior observamos que a estrutura de grupo pode ser definida com base em um conjunto não vazio, munido de uma operação binária e gozando de propriedades específicas. Ao longo desta seção estudaremos a estrutura de anel, observando as semelhanças e as diferenças em relação à estrutura de grupos estudada anteriormente.

Considerando sua função enquanto suporte ao setor de programação de uma indústria de tecnologia e atual encarregado da preparação de um curso de capacitação a um grupo de funcionários, sua primeira tarefa consiste na organização da primeira etapa deste curso de formação voltado ao estudo do conceito de anel e suas principais propriedades, por ser este o principal conceito empregado na fundamentação e elaboração dos algoritmos computacionais por essa empresa.

Para a realização deste curso, você deve elaborar o material que será desenvolvido com os funcionários durante a etapa do curso, inclusive com as explicações a respeito dos conceitos que devem ser estudados pelos funcionários para desenvolver a tarefa proposta e, consequentemente, cumprir as tarefas diárias do setor que integrarão na empresa. Além disso, é necessário que você elabore um gabarito das tarefas que serão propostas, contendo informações detalhadas para auxiliá-lo durante a posterior aplicação do curso.

Nesse sentido, após o desenvolvimento de diversos estudos, foi selecionado o seguinte algoritmo a ser resolvido pelos funcionários durante a primeira etapa da capacitação:

• Considere que um algoritmo implementado em uma máquina que prepara e embala produtos químicos possui as seguintes características:

(a) o operador da máquina insere valores a e b, os quais correspondem às concentrações de dois produtos químicos A e B, respectivamente.

(b) a partir dos dados inseridos, o algoritmo determina o elemento $c = -a$, que é associado à embalagem que deve ser adotada.

(c) a concentração *x* de um terceiro produto químico a ser acrescido na mistura é identificado a partir da expressão $x + a = b$.

Nessa situação, para que não ocorram erros na produção, aos valores a e b devem ser associados números c e x únicos, conforme a descrição anterior.

A partir da situação apresentada, os funcionários precisarão investigar as seguintes questões:

a) Considerando o conjunto dos números naturais com suas operações usuais, os passos descritos nos itens (b) e (c) poderiam ser realizados? Justifique sua resposta com base no conceito de anel e em suas propriedades.

b) Se em vez de tomar os naturais fosse considerado o conjunto dos números inteiros e suas operações usuais, os passos descritos nos itens (b) e (c) poderiam ser realizados? Justifique sua resposta com base no conceito de anel e em suas propriedades.

c) Demonstre a unicidade dos elementos *c* e *x* a partir do anel dos reais, considerando as operações de adição e multiplicação usuais.

Como você poderá auxiliar os funcionários da empresa no desenvolvimento dessa proposta? Resolva a tarefa apresentada de forma detalhada e elabore um texto identificando as respostas esperadas aos questionamentos apresentados e as possíveis dúvidas que podem ser apresentadas pelos funcionários, além de destacar quais conceitos são necessários para a resolução do problema proposto, compondo parte do plano de treinamento a ser elaborado.

Não pode faltar

Historicamente observamos que ocorreu um desenvolvimento tardio da álgebra em relação à sua estruturação lógica e axiomática (DOMINGUES; IEZZI, 2003), quando comparamos com o estudo dos conceitos da geometria, por exemplo, o qual foi realizado desde a Antiguidade, de modo que a formalização das estruturas algébricas, como a estrutura de anel, ocorreu apenas por volta dos séculos XIX e XX.

Saiba mais

"Pelas mãos da escola de Hilbert em Göttingen, e em particular por Emmy Noether, toda a área [da Álgebra] foi colocada sobre fundações axiomáticas. Junto com os grupos, três outros tipos de sistema algébrico foram definidos por uma apropriada lista de axiomas: anéis, campos e álgebras. [...] Há dezenas, talvez centenas, de tipos diferentes de estrutura algébrica, cada um com sua própria lista de axiomas. Alguns foram inventados simplesmente para explorar as consequências de axiomas interessantes, mas a maioria surgiu porque eram necessários em algum problema específico." (STEWART, 2014, p.181-182)

Uma das principais representantes do estudo dos anéis foi Emmy Amalie Noether (1882-1935), a qual, em 1921, publicou um artigo a respeito dessa teoria, adotando uma perspectiva axiomática abstrata (STEWART, 2014).

Vamos agora analisar a estrutura de anel observando as propriedades correspondentes.

Estrutura de anel

Considere um conjunto não vazio A sobre o qual são definidas duas operações fechadas $+$ e $\cdot$ em A, de modo a compor uma terna $(A,+,\cdot)$. Dizemos que a estrutura $(A,+,\cdot)$ corresponde a um **anel** se gozar das seguintes propriedades:

- Para a operação $+$, considerando $x,y,z \in A$ quaisquer, são válidas as propriedades:
  - Associatividade: $x+(y+z)=(x+y)+z$
  - Comutatividade: $x+y=y+x$
  - Elemento neutro: existe $e \in A$ tal que $e+x=x+e=x$
    Elemento simétrico: para todo $x \in A$ existe $-x \in A$ com $x+(-x)=(-x)+x=e$
- Para a operação $\cdot$, sendo $x,y,z \in A$ quaisquer, é válida a:
  - Associatividade: $x\cdot(y\cdot z)=(x\cdot y)\cdot z$
- Para ambas as operações, para todos $x,y,z \in A$, é válida a:
  - Distributividade de $\cdot$ em relação à $+$: $x\cdot(y+z)=x\cdot y+x\cdot z$ e $(y+z)\cdot x=y\cdot x+z\cdot x$.

Assimile

Em suma, a estrutura $(A,+,\cdot)$ será classificada como **anel** quando $(A,+)$ for um grupo abeliano, $(A,\cdot)$ gozar da associatividade e a propriedade distributiva de $\cdot$ em relação à $+$ for válida.

Dentre os principais conjuntos numéricos, os quais são estudados desde a Educação Básica, munidos de suas operações usuais de adição e multiplicação, podemos construir os seguintes anéis: $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ e $(\mathbb{C},+,\cdot)$.

Note, por exemplo, que $(\mathbb{R},+,\cdot)$ é um anel. De fato, as operações de adição e multiplicação são fechadas no conjunto de números reais. Além disso, $(\mathbb{R},+)$ é um grupo abeliano, conforme estudado anteriormente. Também temos que a multiplicação em $\mathbb{R}$ é associativa, pois para todos $x,y,z\in\mathbb{R}$ é possível verificar que $x\cdot(y\cdot z)=(x\cdot y)\cdot z$. A distributividade da multiplicação em relação à adição é também válida quando consideramos ambas as operações definidas em $\mathbb{R}$, pois, para todos $x,y\in\mathbb{R}$ podemos verificar que $x(y+z)=xy+xz$ e $(y+z)x=yx+zx$. Portanto, $(\mathbb{R},+,\cdot)$ pode ser classificado como anel.

Podemos empregar argumentos análogos para provar que $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$ e $(\mathbb{C},+,\cdot)$ são anéis.

Além disso, com base nos conjuntos numéricos, podemos construir outros anéis, como a estrutura apresentada no exemplo a seguir.

Exemplificando

Considere o conjunto $P=\left\{a+b\sqrt{2}\;\middle|\;a,b\in\mathbb{Z}\right\}$, sobre o qual podemos definir operações de adição e multiplicação correspondentes da seguinte forma: para $a+b\sqrt{2}$ e $c+d\sqrt{2}$ pertencentes à P, temos que:

- Adição:

$$\left(a+b\sqrt{2}\right)+\left(c+d\sqrt{2}\right)=(a+c)+(b+d)\sqrt{2}$$

- Multiplicação:

$$\left(a+b\sqrt{2}\right)\left(c+d\sqrt{2}\right)=(ac+2bd)+(ad+bc)\sqrt{2}$$

Temos que $(P,+,\cdot)$ é um anel. De fato, as operações de adição e multiplicação são fechadas em P, isto é, se $x,y \in P$, então $x+y \in P$ e $xy \in P$. Vamos verificar que $(P,+)$ é um grupo abeliano. A propriedade associativa é válida, pois tomando $x=a+b\sqrt{2}$, $y=c+d\sqrt{2}$ e $z=e+f\sqrt{2} \in P$, note que

$$x+y=\left(a+b\sqrt{2}\right)+\left(c+d\sqrt{2}\right)=(a+c)+(b+d)\sqrt{2}$$

$$y+z=\left(c+d\sqrt{2}\right)+\left(e+f\sqrt{2}\right)=(c+e)+(d+f)\sqrt{2}$$

e, assim,

$$\begin{aligned}(x+y)+z&=\left[(a+c)+(b+d)\sqrt{2}\right]+\left(e+f\sqrt{2}\right)\\&=\left[(a+c)+e\right]+\left[(b+d)+f\right]\sqrt{2}\\&=\left[a+(c+e)\right]+\left[b+(d+f)\right]\sqrt{2}\\&=\left(a+b\sqrt{2}\right)+\left[(c+e)+(d+f)\sqrt{2}\right]\\&=x+(y+z)\end{aligned}$$

o que implica na validade da associatividade em $(P,+)$. A propriedade comutativa é verificada, pois para $x=a+b\sqrt{2}$, $y=c+d\sqrt{2} \in P$ temos

$$\begin{aligned}x+y&=\left(a+b\sqrt{2}\right)+\left(c+d\sqrt{2}\right)\\&=(a+c)+(b+d)\sqrt{2}\\&=(c+a)+(d+b)\sqrt{2}\\&=\left(c+d\sqrt{2}\right)+\left(a+b\sqrt{2}\right)=y+x\end{aligned}$$

O elemento neutro referente à adição é $0=0+0\sqrt{2} \in P$, de modo que para todo $x=a+b\sqrt{2} \in P$, é válido que

$$x+0=\left(a+b\sqrt{2}\right)+\left(0+0\sqrt{2}\right)=(a+0)+(b+0)\sqrt{2}=a+b\sqrt{2}=x$$

$$0+x=\left(0+0\sqrt{2}\right)+\left(a+b\sqrt{2}\right)=(0+a)+(0+b)\sqrt{2}=a+b\sqrt{2}=x$$

isto é, $x+0=0+x=x$ para todo $x\in P$.

A cada elemento $x=a+b\sqrt{2}\in P$, temos o simétrico $-x=-a+(-b)\sqrt{2}\in P$, de modo que

$$\begin{aligned}x+(-x)&=\left(a+b\sqrt{2}\right)+\left[(-a)+(-b)\sqrt{2}\right]\\&=\left[a+(-a)\right]+\left[b+(-b)\right]\sqrt{2}=0+0\sqrt{2}=0\end{aligned}$$

$$\begin{aligned}(-x)+x&=\left[(-a)+(-b)\sqrt{2}\right]+\left(a+b\sqrt{2}\right)\\&=\left[(-a)+a\right]+\left[(-b)+b\right]\sqrt{2}=0+0\sqrt{2}=0\end{aligned}$$

Além disso, note que a multiplicação é associativa em $(P,+,\cdot)$, pois para todos $x=a+b\sqrt{2}$, $y=c+d\sqrt{2}$ e $z=e+f\sqrt{2}\in P$, note que

$$x\cdot y=\left(a+b\sqrt{2}\right)\cdot\left(c+d\sqrt{2}\right)=(ac+2bd)+(ad+bc)\sqrt{2}$$

$$y\cdot z=\left(c+d\sqrt{2}\right)\cdot\left(e+f\sqrt{2}\right)=(ce+2df)+(cf+de)\sqrt{2}$$

assim,

$$\begin{aligned}(x\cdot y)\cdot z&=\left[(ac+2bd)+(ad+bc)\sqrt{2}\right]\cdot\left(e+f\sqrt{2}\right)\\&=\left[(ac+2bd)e+2(ad+bc)f\right]+\left[(ac+2bd)f+(ad+bc)e\right]\sqrt{2}\\&=\left[(ace+2bde)+(2adf+2bcf)\right]+\left[(acf+2bdf)+(ade+bce)\right]\sqrt{2}\\&=\left[a(ce+2df)+2b(de+cf)\right]+\left[a(cf+de)+b(2df+ce)\right]\sqrt{2}\\&=\left[a(ce+2df)+2b(cf+de)\right]+\left[a(cf+de)+b(ce+2df)\right]\sqrt{2}\\&=\left(a+b\sqrt{2}\right)\cdot\left[(ce+2df)+(cf+de)\sqrt{2}\right]\\&=x\cdot(y\cdot z)\end{aligned}$$

A propriedade distributiva da multiplicação em relação à adição é também válida em $(P,+,\cdot)$, pois para todos $x=a+b\sqrt{2}$, $y=c+d\sqrt{2}$ e $z=e+f\sqrt{2}\in P$ temos que

$$
\begin{aligned}
(x+y)\cdot z &= \left[(a+c)+(b+d)\sqrt{2}\right]\cdot\left(e+f\sqrt{2}\right)\\
&= \left[(a+c)e+2(b+d)f\right]+\left[(a+c)f+(b+d)e\right]\sqrt{2}\\
&= \left[(ae+ce)+2(bf+df)\right]+\left[(af+cf)+(be+de)\right]\sqrt{2}\\
&= (ae+ce)+2(bf+df)+(af+cf)\sqrt{2}+(be+de)\sqrt{2}\\
&= \left[(ae+2bf)+(af+be)\sqrt{2}\right]+\left[(ce+2df)+(cf+de)\sqrt{2}\right]\\
&= \left[\left(a+b\sqrt{2}\right)\left(e+f\sqrt{2}\right)\right]+\left[\left(c+d\sqrt{2}\right)\left(e+f\sqrt{2}\right)\right]\\
&= x\cdot z+y\cdot z
\end{aligned}
$$

De modo análogo, podemos verificar que $x\cdot(y+z)=x\cdot y+x\cdot z$. Portanto, $(P,+,\cdot)$ pode ser classificado como anel.

Podemos generalizar a estrutura apresentada no exemplo anterior construindo o conjunto $\mathbb{Z}[p]=\left\{a+b\sqrt{p}\;\middle|\; a,b\in\mathbb{Z},\ p \text{ primo}\right\}$ sobre o qual podemos definir duas operações, uma adição e uma multiplicação, análogas às operações apresentadas no exemplo anterior. Assim, temos que $(\mathbb{Z}[p],+,\cdot)$ pode ser classificado como anel, para *p* primo.

Faça você mesmo

Seja o conjunto $K=\left\{x+y\sqrt{3}\;\middle|\; x,y\in\mathbb{Z}\right\}$, sobre o qual podemos definir operações de adição e multiplicação dadas para $a+b\sqrt{3}$ e $c+d\sqrt{3}$ pertencentes à *K*, por:

• Adição:

$$\left(a+b\sqrt{3}\right)+\left(c+d\sqrt{3}\right)=(a+c)+(b+d)\sqrt{3}$$

• Multiplicação:

$$\left(a+b\sqrt{3}\right)\left(c+d\sqrt{3}\right)=(ac+3bd)+(ad+bc)\sqrt{3}$$

Mostre que $(K,+,\cdot)$ pode ser classificado como um anel.

Note que a estrutura $(\mathbb{N},+,\cdot)$, construída a partir do conjunto dos números naturais, não é um anel. Com efeito, com as operações de adição e multiplicação usuais definidas sobre $\mathbb{N}$, são verificadas as propriedades do fechamento, associatividade e distributividade da multiplicação em relação à adição. Temos que a adição é comutativa e goza da existência de elemento neutro para a adição, o qual corresponde ao zero em $\mathbb{N}$. No entanto, $(\mathbb{N},+,\cdot)$ não possui a propriedade da existência de elemento simétrico relativo à adição (oposto) para todo número natural, visto que basta verificar que o número $7 \in \mathbb{N}$ possui como oposto o número -7, que não pertence ao conjunto dos números naturais. Como uma das propriedades da definição de anel não pode ser verificada, podemos concluir que $(\mathbb{N},+,\cdot)$ não é um anel.

Assim, para que uma estrutura $(A,+,\cdot)$ seja classificada como anel, é necessário que ela possua todas as propriedades presentes na definição de anel, simultaneamente. Se uma delas não for verificada, temos que a estrutura não caracterizará um anel.

Considere um anel $(A,+,\cdot)$. Além das propriedades que compõem sua definição, podemos ainda identificar propriedades que decorrem da definição.

Propriedades imediatas da definição

Sabemos que se $(A,+,\cdot)$ é um anel, então $(A,+)$ é um grupo abeliano. Desse fato, as seguintes propriedades podem ser verificadas, conforme estudado na unidade anterior:

• Propriedade 1: o elemento neutro e referente à operação $+$ do anel $(A,+,\cdot)$ é único, pois corresponde ao elemento neutro de $(A,+)$.

• Propriedade 2: para todo $x \in A$, o simétrico de $-x$, em relação à operação $+$, é o próprio x, isto é, $-(-x) = x$.

• Propriedade 3: para todos $x,y,a \in A$, se $x + a = y + a$, então $x = y$, ou seja, é válida a lei do cancelamento para o operação $+$.

Considerando a operação de multiplicação são válidas as seguintes propriedades:

• Propriedade 4: para todo $x \in A$ é válido que $x \cdot e = e \cdot x = e$, em que e corresponde ao elemento neutro da operação $+$.

De fato, para todo $x \in A$, temos que $e \cdot x \in A$ e $x \cdot e \in A$ porque $(A,+,\cdot)$ é um anel e goza do fechamento para a operação $\cdot$. Como e é elemento neutro da adição, e a estrutura $(A,+,\cdot)$ goza da distributividade de $\cdot$ em relação à $+$, segue que $e + x \cdot e = x \cdot e = x \cdot (e + e) = x \cdot e + x \cdot e$, o que, pela lei do cancelamento para a operação $+$, implica em $e = x \cdot e$. Por outro lado, se $e + e \cdot x = e \cdot x = (e + e) \cdot x = e \cdot x + e \cdot x$, o que, também pela lei do cancelamento, implica $e = e \cdot x$, o que comprova a propriedade.

- Propriedade 5: para todos $x, y \in A$ é válido que $(-x) \cdot y = x \cdot (-y) = -(x \cdot y)$.

Assim, considerando $x, y \in A$ quaisquer, como $(A,+,\cdot)$ é um anel, essa estrutura goza do fechamento para a operação $\cdot$, existência de elemento neutro e em relação a operação $+$ e existência de elemento simétrico $-x$ para todo $x \in A$, relativos à operação $+$, a distributividade da operação $\cdot$ em relação à $+$.

Com base nessas propriedades, e na propriedade 4, segue que

$$x \cdot y + [-(x \cdot y)] = e = x \cdot e = x \cdot [y + (-y)] = x \cdot y + x \cdot (-y)$$

Pela lei do cancelamento podemos concluir que $-(x \cdot y) = x \cdot (-y)$. Por outro lado, temos que

$$x \cdot y + [-(x \cdot y)] = e = e \cdot y = [x + (-x)] \cdot y = x \cdot y + (-x) \cdot y$$

o que também, pela lei do cancelamento, implica em $-(x \cdot y) = (-x) \cdot y$, comprovando, assim, a validade da propriedade $(-x) \cdot y = x \cdot (-y) = -(x \cdot y)$ para todos $x, y \in A$.

- Propriedade 6: para todos $x, y \in A$ é válido que $x \cdot y = (-x) \cdot (-y)$.

De fato, para $x, y \in A$ quaisquer, das propriedades 2 e 5 temos que $(-x) \cdot (-y) = -[(-x) \cdot y] = -[-(x \cdot y)] = x \cdot y$. Logo, $(-x) \cdot (-y) = x \cdot y$ para todos $x, y \in A$.

Reflita

Considerando o conjunto dos números inteiros munido da operação usual de multiplicação, como podemos justificar a "regra de sinal" na Educação Básica? Que tipos de recursos podem ser empregados para auxiliar no ensino desse conteúdo?

Em um anel $(A,+,\cdot)$ podemos ainda definir a diferença entre elementos com base na propriedade da existência de elemento simétrico para todo elemento de *A*.

Dessa forma, considere um anel $(A,+,\cdot)$. Se $x,y \in A$, podemos definir a **diferença** entre *x* e *y*, denotada por $x-y$, como o elemento $x+(-y)$, isto é, $x-y=x+(-y)$.

Por exemplo, no conjunto de números reais, munido das operações usuais de adição e multiplicação, temos que a diferença entre números reais *x* e *y* é dada por $x-y=x+(-y)$, o que possibilita a estruturação da operação de subtração definida sobre o conjunto.

Considerando a definição da diferença entre elementos de um anel $(A,+,\cdot)$, dados $a,x,y \in A$, podemos verificar que $a\cdot(x-y)=a\cdot x-a\cdot y$, pois

$$a\cdot(x-y)=a\cdot[x+(-y)]=a\cdot x+a\cdot(-y)=a\cdot x+[-(a\cdot y)]=a\cdot x-a\cdot y$$

Fato este que decorre da propriedade 7, apresentada anteriormente, e da distributividade, ambas válidas no anel $(A,+,\cdot)$.

Faça você mesmo

Mostre que a expressão $(x-y)\cdot a=x\cdot a-y\cdot a$ é válida para todos $a,x,y \in A$, em que $(A,+,\cdot)$ pode ser classificado como anel.

Pesquise mais

Para complementar os estudos a respeito da estrutura de anel, consulte a seção 1.5 do livro *Estruturas Algébricas*, de Julio Cesar Cochmanski e Liliane Cristina de Camargo Cochmanski, disponível em sua biblioteca virtual.

Sem medo de errar

Como funcionário de uma indústria de tecnologia, você foi designado para preparar um curso de capacitação para uma equipe que atuará, assim como você, como suporte ao setor de programação. Sua primeira responsabilidade é organizar as tarefas a serem propostas na primeira etapa do curso em relação ao estudo

do conceito de anel e suas principais propriedades, por se tratar do principal conteúdo teórico utilizado na fundamentação dos algoritmos computacionais elaborados pela empresa.

Foi selecionado, para a primeira etapa do curso, o estudo de um algoritmo que envolve, dentre outras ações, a identificação de um elemento $c = -a$, referente ao passo (b) do algoritmo, e de um elemento *x* com base na expressão $x + a = b$, correspondente ao passo (c) desse mesmo algoritmo, informações analisadas a partir de valores a e b inseridos pelo operador da máquina. Além disso, sabe-se que, para que não ocorram erros na produção, os números *c* e *x* devem ser únicos.

Considere o conjunto dos números naturais munido das operações usuais de adição e multiplicação, compondo a estrutura $(\mathbb{N}, +, \cdot)$. Note que para a determinação de *c*, devemos identificar o elemento simétrico de *a* em relação a operação de adição, ou seja, o elemento $-a$. No entanto, na estrutura $(\mathbb{N}, +, \cdot)$, a propriedade da existência de elemento simétrico a todo elemento de $\mathbb{N}$, em relação à adição, ou seja, do oposto, não é verificada porque o oposto do número 2 corresponde ao -2, o qual não pertence a $\mathbb{N}$, por exemplo. Por outro lado, na determinação de *x*, também faz-se necessário identificar o oposto ao elemento a, pois a resolução da equação $x + a = b$ envolve o emprego das propriedades de existência de elemento neutro e de elemento simétrico para a adição, sendo a última não é verificada em $(\mathbb{N}, +, \cdot)$. Como $(\mathbb{N}, +, \cdot)$ não é anel, porque não goza de uma das propriedades necessárias (a existência de elemento simétrico a todo elemento de $\mathbb{N}$ em relação à operação $+$), podemos concluir que os passos (b) e (c) do algoritmo não podem ser executados em $(\mathbb{N}, +, \cdot)$.

Porém, quando consideramos a estrutura $(\mathbb{Z}, +, \cdot)$, a qual pode ser classificada como anel, os passos (b) e (c) podem ser empregados. De fato, o par $(\mathbb{Z}, +)$ pode ser classificado como um grupo abeliano, conforme discutido na unidade anterior, já que a adição é fechada em $\mathbb{Z}$ porque a soma de inteiros resulta em um inteiro. A adição é também associativa e comutativa, pois para todos $x, y, z \in \mathbb{Z}$ é válido, respectivamente, que $x + (y + z) = (x + y) + z$ e $x + y = y + x$. O elemento neutro da adição é o zero, pois $x + 0 = 0 + x = x$ para todo x inteiro. Além disso, se $x \in \mathbb{Z}$, seu simétrico em relação à adição (ou oposto) é o número $-x \in \mathbb{Z}$. A estrutura $(\mathbb{Z}, \cdot)$ goza do fechamento, porque o

produto de inteiros é um número inteiro e da associatividade, pois para $x, y, z \in \mathbb{Z}$ temos que $x \cdot (y \cdot z) = (x \cdot y) \cdot z$. Por fim, $(\mathbb{Z}, +, \cdot)$ goza da propriedade distributiva da multiplicação em relação à adição, pois tomando $x, y, z \in \mathbb{Z}$, verifica-se $x \cdot (y + z) = x \cdot y + x \cdot z$ e $(y + z) \cdot x = y \cdot x + z \cdot x$. Sendo assim, $(\mathbb{Z}, +, \cdot)$ é um anel.

Como $(\mathbb{Z}, +, \cdot)$ é um anel, o elemento $c = -a$ pode ser identificado, porque corresponde ao simétrico de a em relação à adição, propriedade que é verificada em $\mathbb{Z}$. Podemos identificar *x* que satisfaz a equação $x + a = b$, pois pelas propriedades da associatividade, existência de elemento neutro e simétrico, válidas em $(\mathbb{Z}, +)$ e, consequentemente, em $(\mathbb{Z}, +, \cdot)$, segue que

$$\begin{aligned} x + a = b &\Rightarrow (x + a) + (-a) = b + (-a) \\ &\Rightarrow x + [a + (-a)] = b + (-a) \\ &\Rightarrow x + 0 = b + (-a) \\ &\Rightarrow x = b + (-a) \end{aligned}$$

Assim, *x* é tal que $x = b + (-a)$. Portanto, na estrutura $(\mathbb{Z}, +, \cdot)$, os passos (b) e (c) do algoritmo podem ser executados.

A última tarefa consiste em demonstrar a unicidade dos elementos *c* e *x*, presentes no algoritmo computacional. Assim, para justificar essas afirmações, precisamos comprovar a unicidade do elemento simétrico de qualquer inteiro *a*, pois $c = -a$, bem como demonstrar que a equação $x + a = b$ tem solução única em $\mathbb{Z}$, sendo $a, b \in \mathbb{Z}$, o que garante a unicidade de *x*, o qual pode ser dado por $x = b + (-a)$. Vamos comprovar a validade de cada uma dessas afirmações.

• Para cada elemento $a \in \mathbb{Z}$ existe um único simétrico relativo à operação usual de adição de inteiros.

Seja $a \in \mathbb{Z}$. Suponha que existam dois elementos $x, y \in \mathbb{Z}$ simétricos ao número a em relação à adição, ou seja, $a + x = x + a = 0$ e $a + y = y + a = 0$. Dessa forma,

$$x = x + 0 = x + (a + y) = (x + a) + y = 0 + y = y$$

Logo, o elemento simétrico, em relação à adição, associado a cada $a \in \mathbb{Z}$, é único.

• Se $a,b \in \mathbb{Z}$, então a equação $x + a = b$ tem uma única solução em $\mathbb{Z}$, a qual é dada por $x = b + (-a)$.

Considere a equação $x + a = b$. Note que $x = b + (-a)$ é solução da equação apresentada, pois substituindo essa expressão na equação em estudo, sabendo que $(\mathbb{Z}, +, \cdot)$ é um anel, temos

$$[b + (-a)] + a = b + [(-a) + a] = b + 0 = b$$

Além disso, se $x_0 \in \mathbb{Z}$ é uma solução da equação, então $x_0 + a = b$, o que implica em

$$\begin{aligned} x_0 + a = b &\Rightarrow (x_0 + a) + (-a) = b + (-a) \\ &\Rightarrow x_0 + [a + (-a)] = b + (-a) \\ &\Rightarrow x_0 + 0 = b + (-a) \\ &\Rightarrow x_0 = b + (-a) \end{aligned}$$

Ou seja, se $x_0 \in \mathbb{Z}$ é solução da equação $x + a = b$, então $x_0 = b + (-a)$, o que acarreta na unicidade da solução da equação estudada.

Para finalizar sua tarefa na primeira etapa do curso, elabore um documento contendo o enunciado das tarefas que devem ser desenvolvidas pelos funcionários. Elabore também um documento contendo as resoluções detalhadas para as tarefas propostas, indicando os conceitos necessários a serem desenvolvidos para que os funcionários possam executar as propostas, e possíveis dúvidas que podem surgir ao longo desses estudos.

Avançando na prática

Relação entre o conjunto dos números inteiros e o conjunto de números complexos

Descrição da situação-problema

Imagine que você é um professor da Educação Básica e quer desenvolver um trabalho a respeito dos números complexos com uma turma do Ensino Médio. Para isso, você pretende aprofundar seus estudos de modo a adequar os conceitos e a linguagem que

serão empregados a fim de atender o nível dos alunos e associar com seus conhecimentos a respeito dos demais conjuntos numéricos.

Historicamente, um dos principais matemáticos que desenvolveu estudos a respeito dos números inteiros negativos e dos complexos foi Johann Carl Friedrich Gauss (1777-1855). Seus trabalhos contribuíram, dentre outros, para a estruturação do conjunto de números complexos. Os números inteiros podem ser associados aos números complexos a partir do conjunto conhecido como anel dos inteiros de Gauss $(Z[i],+,\cdot)$, com $\mathbb{Z}[i]=\{a+bi \mid a,b\in\mathbb{Z}\}$. Sobre este conjunto, podemos definir uma adição $+$ e uma multiplicação $\cdot$, de modo que se $x=a+bi$ e $y=c+di$ pertencem a $\mathbb{Z}[i]$, então $x+y=(a+c)+(b+d)i\in\mathbb{Z}[i]$ e $x\cdot y=(ac-bd)+(ad+bc)i\in\mathbb{Z}[i]$, que são as operações de $\mathbb{C}$ restritas a $\mathbb{Z}[i]$.

Como você justificaria que a estrutura $(\mathbb{Z}[i],+,\cdot)$ pode ser classificada como anel? Quais as contribuições do conhecimento da estrutura do anel dos inteiros de Gauss para o trabalho com o conjunto de números complexos na Educação Básica? Se a estrutura $(\mathbb{Z}[i],+,\cdot)$ não satisfizesse, por exemplo, a propriedade do fechamento de ambas as operações, de que forma esse fato influenciaria no trabalho com o conjunto dos números complexos na Educação Básica?

Resolução da situação-problema

Podemos observar que as operações de adição e multiplicação definidas sobre $\mathbb{Z}[i]$ são fechadas, pois correspondem a restrições das operações definidas em $\mathbb{C}$ sobre $\mathbb{Z}[i]$. $(\mathbb{Z}[i],+)$, um grupo abeliano, porque, para todos $x,y,z\in\mathbb{Z}[i]$, é verificada a associatividade, já que $(x+y)+z=x+(y+z)$, a comutatividade, porque é válido que $x+y=y+x$, a existência de elemento neutro, o qual corresponde a $0=0+0i\in\mathbb{Z}[i]$ e satisfaz a expressão $x+0=0+x=x$, e a existência de elemento simétrico, que a cada $x=a+bi\in\mathbb{Z}[i]$ é descrito por $-x=-a+(-b)i\in\mathbb{Z}[i]$ com $x+(-x)=(-x)+x=0$. A multiplicação é associativa em $(\mathbb{Z}[i],+,\cdot)$, pois para todos $x,y,z\in\mathbb{Z}[i]$ é válido que $(x\cdot y)\cdot z=x\cdot(y\cdot z)$. A propriedade distributiva da multiplicação em relação à adição é também válida em $(\mathbb{Z}[i],+,\cdot)$, pois para todos $x,y,z\in\mathbb{Z}[i]$, com base na associatividade e na comutatividade de

ambas as operações, bem como a distributividade da multiplicação em relação à adição em $(\mathbb{Z},+,\cdot)$, temos que $(x+y)\cdot z = x\cdot z + y\cdot z$ e $x\cdot(y+z) = x\cdot y + x\cdot z$. Portanto, $(\mathbb{Z}[i],+,\cdot)$ é um anel.

Devido a $(\mathbb{Z}[i],+,\cdot)$ gozar das propriedades que definem um anel, esta estrutura pode ser empregada na resolução de problemas que envolvem os números complexos cuja parte real e imaginária são descritas por números inteiros, sendo estes os principais exemplos de números complexos abordados na Educação Básica. Em geral, quando organizamos propostas para a Educação Básica voltadas à aprendizagem do conjunto de números complexos, adotamos os principais exemplos como os números na forma $x = a + bi$ com *a* e *b* inteiros. Essa opção também pode ser observada nos materiais didáticos, por exemplo no estudo da representação dos números complexos no plano complexo, análogo ao estudo dos pontos no plano cartesiano. Assim, esse tipo de trabalho pode auxiliar os alunos na diferenciação entre as partes real e imaginária de um número complexo, empregando as propriedades dos números inteiros que são estudadas desde o Ensino Fundamental e com as quais os alunos já estão acostumados a trabalhar. Se na estrutura $(\mathbb{Z}[i],+,\cdot)$ as operações correspondentes não fossem fechadas, na Educação Básica não poderíamos, por exemplo, propor atividades que envolvessem o cálculo da soma ou do produto envolvendo os números complexos $x = 2 + 3i$ e $y = -1 + 5i$ e suas representações no plano complexo, já que os resultados poderiam ser números que não admitissem uma representação desse tipo. Ou ainda, empregar os números complexos na resolução de problemas como o estudo das raízes complexas de equações polinomiais. Portanto, o conhecimento da estrutura de anel pode favorecer o trabalho do professor no sentido de contribuir com a elaboração de propostas que sejam válidas e que, ao mesmo tempo, contribuam com a aprendizagem dos alunos.

Faça valer a pena

1. Um estudante precisa comprovar que um conjunto *L* não vazio, sobre o qual são definidas operações de adição $(+)$ e multiplicação $(\cdot)$, ambas fechadas em *L*, pode ser classificado como anel.

Durante seus estudos, o estudante já comprovou a validade das seguintes propriedades:

I. Associatividade da multiplicação.
II. Comutatividade da adição.
III. Distributividade da multiplicação em relação à adição.
IV. Existência de elemento neutro da adição.

Assinale a alternativa que indica propriedades que também devem ser analisadas pelo estudante para justificar que $(L,+,\cdot)$ é um anel.

a) Existência de elemento neutro em relação à multiplicação e associatividade da adição.
b) Comutatividade da multiplicação e existência de elemento neutro em relação à multiplicação.
c) Associatividade da adição e existência de elemento simétrico para todo elemento de *L* em relação à adição.
d) Comutatividade da multiplicação e associatividade da adição.
e) Existência de elemento simétrico para todo elemento de *L* em relação à multiplicação e comutatividade da multiplicação.

2. A partir do conjunto dos números inteiros, considerando as operações usuais de adição e multiplicação, existe um conjunto de propriedades que podem ser verificadas, devido à possibilidade de caracterização dessa estrutura como anel. Além dessa, outras estruturas podem ser classificadas como anéis devido ao fato de satisfazerem ao mesmo conjunto de propriedades verificado em $(\mathbb{Z},+,\cdot)$, adequando-as às suas operações características.
Considere que um problema esteja sendo resolvido com base em um anel $(T,+,\cdot)$ que goza também da comutatividade da operação $\cdot$. Suponha também que nenhuma outra propriedade seja verificada em $(T,+,\cdot)$ além das propriedades próprias de um anel e a comutatividade da operação $\cdot$.

Sendo $x,y,z \in T$ elementos quaisquer do conjunto, assinale a alternativa que indica a única expressão que será sempre válida considerando as propriedades que são verificadas no anel $(T,+,\cdot)$:

a) $(x+y)\cdot z = x\cdot z + y\cdot x$.
b) $x+y\cdot z = x\cdot y + z$.
c) $x\cdot z + z\cdot y = x\cdot y\cdot z$.
d) $x\cdot y + x\cdot z = y\cdot z$.
e) $z\cdot y + x\cdot z = (x+y)\cdot z$.

3. Considere $A = 2\mathbb{Z}$ o conjunto composto pelos números inteiros pares, o qual é um subconjunto de $\mathbb{Z}$. Sobre esse conjunto podemos definir as operações usuais de adição $(+)$ e multiplicação $(\cdot)$ de inteiros, ou seja, restringir as operações usuais de $\mathbb{Z}$ sobre *A*.
Em relação a esse conjunto com as operações correspondentes, analise as seguintes afirmações e a relação proposta entre elas:
I. A estrutura $(A, +, \cdot)$ pode ser classificada como anel.

PORQUE

II. A estrutura $(A, \cdot)$ goza da propriedade da existência de elemento neutro.

A respeito das afirmações apresentadas, assinale a alternativa correta.

a) As afirmações I e II estão corretas, e a II é uma justificativa correta para a I.
b) As afirmações I e II estão corretas, mas a II não é uma justificativa correta para a I.
c) A afirmação I está correta e a II incorreta.
d) A afirmação II está correta e a I incorreta.
e) As afirmações I e II estão incorretas.

Seção 3.2

Anéis comutativos e anéis com unidade

Diálogo aberto

Na seção anterior discutimos a respeito da estrutura de anel, uma das principais estruturas algébricas estudada pela Álgebra Abstrata. Um anel é uma estrutura composta por um conjunto não vazio com duas operações binárias que gozam de propriedades específicas. Nesta seção estudaremos a respeito de algumas categorias importantes de anéis, como os anéis comutativos e os anéis com unidade, bem como os subanéis e alguns exemplos importantes.

Considere que na segunda etapa do curso de capacitação para os funcionários da empresa de tecnologia, os cursistas deverão resolver um problema envolvendo um algoritmo elaborado para uma máquina que efetua cortes para a confecção de embalagens para diversos produtos. Para a resolução deste problema, além dos conhecimentos a respeito das propriedades dos anéis, é fundamental o conhecimento a respeito do conjunto de matrizes, suas operações e propriedades específicas.

Com base nesse contexto, nesta seção, você deverá elaborar os materiais que serão utilizados na segunda etapa da capacitação, incluindo as tarefas, a forma que serão propostas aos funcionários, bem como as resoluções comentadas e o levantamento sobre possíveis dúvidas que podem surgir durante a capacitação para que você possa se preparar para a aplicação dessa segunda etapa do curso.

O problema a ser resolvido pelos funcionários parte da seguinte situação: um dos algoritmos computacionais empregado no funcionamento de uma máquina para corte de embalagens emprega matrizes quadradas de ordem 2 para o armazenamento e exibição dos dados, bem como para a realização dos cálculos. Nos cálculos empregados para a execução do algoritmo são empregadas as operações usuais de adição e multiplicação de matrizes, além de suas propriedades características. Visando um aprofundamento no estudo do conjunto apresentado anteriormente, nesta etapa os

funcionários precisarão demonstrar que o conjunto apresentado, com suas operações usuais, o qual é empregado no algoritmo para a máquina de cortes de embalagens, pode ser classificado como um anel. Também eles devem responder aos seguintes questionamentos: a estrutura em questão pode ser classificada como um anel comutativo? E como anel com unidade? Justifique sua resposta, comprovando a validade das propriedades ou apresentando contraexemplos no caso em que as propriedades não forem válidas.

Diante disso, sua tarefa, inicialmente, consiste em resolver os problemas propostos, identificando os principais conhecimentos que os funcionários precisam construir ao longo da capacitação para que possam lidar com este e com outros problemas similares, bem como refletir sobre possíveis dúvidas que possam surgir no decorrer dessa etapa do curso de capacitação. Em seguida, elabore uma tarefa adicional com base no contexto apresentado e que possibilite aos funcionários aplicarem os conhecimentos a respeito dos subanéis. Por fim, organize as tarefas que serão propostas na segunda etapa do curso e construa um texto contendo as resoluções detalhadas para as questões propostas, as orientações em relação aos conhecimentos da estrutura de anel envolvidos em cada parte da resolução, as possíveis dúvidas e encaminhamentos que podem ser tomados no decorrer do curso de capacitação, a fim de que possam auxiliá-lo durante a realização do curso no atendimento às dúvidas dos funcionários.

Não pode faltar

Na seção anterior estudamos que a estrutura $(A,+,\cdot)$ será classificada como anel quando ambas operações forem fechadas em A, quando $(A,+)$ puder ser classificada como um grupo abeliano, quando $(A,\cdot)$ gozar da associatividade e quando a propriedade distributiva da operação $\cdot$ em relação à $+$ em $(A,+,\cdot)$ for válida.

Um exemplo de anel que podemos destacar é o anel das funções reais de uma variável. Para estudá-lo, consideraremos o conjunto $\mathbb{R}^{\mathbb{R}} = \{f \mid f : \mathbb{R} \to \mathbb{R}\}$ composto pelas funções de uma variável real. A partir dele podemos definir as operações usuais de adição e multiplicação de funções como segue: se $f, g \in \mathbb{R}^{\mathbb{R}}$, então $f : \mathbb{R} \to \mathbb{R}$ e $g : \mathbb{R} \to \mathbb{R}$, assim:

•Podemos definir a soma $f+g:\mathbb{R}\to\mathbb{R}$ por $(f+g)(x)=f(x)+g(x)$ para todo $x\in\mathbb{R}$.

• Podemos definir o produto $fg:\mathbb{R}\to\mathbb{R}$ por $(fg)(x)=f(x)g(x)$ para todo $x\in\mathbb{R}$.

Com essas operações, podemos classificar a estrutura $\left(\mathbb{R}^{\mathbb{R}},+,\cdot\right)$ como um anel. De fato, temos por definição que ambas as operações são fechadas em $\mathbb{R}^{\mathbb{R}}$. Veja que $\left(\mathbb{R}^{\mathbb{R}},+\right)$ é um grupo abeliano, porque a propriedade associativa da adição é válida, já que ao considerar $f,g,h\in\mathbb{R}^{\mathbb{R}}$, para todo $x\in\mathbb{R}$ e sabendo da validade da associatividade em $\mathbb{R}$, segue que

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

o que implica na validade da propriedade associativa em $\left(\mathbb{R}^{\mathbb{R}},+\right)$. A propriedade comutativa da adição é verificada, pois $(f+g)(x)=f(x)+g(x)=g(x)+f(x)=(g+f)(x)$ para $f,g\in\mathbb{R}^{\mathbb{R}}$ e $x\in\mathbb{R}$, fato decorrente da comutatividade da adição em $\mathbb{R}$. O elemento neutro referente à adição corresponde à função nula $0\in\mathbb{R}^{\mathbb{R}}$, ou seja, a função $0:\mathbb{R}\to\mathbb{R}$ definida por $0(x)=0$ para todo $x\in\mathbb{R}$, pois para toda $f\in\mathbb{R}^{\mathbb{R}}$ e todo $x\in\mathbb{R}$, temos $(f+0)(x)=f(x)+0(x)=f(x)+0=f(x)$ e $(0+f)(x)=0(x)+f(x)=0+f(x)=f(x)$. Logo, a propriedade da existência de elemento neutro é verificada em $\left(\mathbb{R}^{\mathbb{R}},+\right)$, sendo $0\in\mathbb{R}^{\mathbb{R}}$ seu elemento neutro. Considerando esse elemento neutro, a cada função $f\in\mathbb{R}^{\mathbb{R}}$ podemos identificar $-f\in\mathbb{R}^{\mathbb{R}}$, tal que $(-f)(x)=-f(x)$ para todo $x\in\mathbb{R}$, a qual satisfaz

$$\big[f+(-f)\big](x)=f(x)+(-f)(x)=f(x)+\big[-f(x)\big]=0$$

$$\big[(-f)+f\big](x)=(-f)(x)+f(x)=\big[-f(x)\big]+f(x)=0$$

sendo comprovada a validade da existência de elemento simétrico, que nesse caso pode ser chamado de oposto a toda função $f\in\mathbb{R}^{\mathbb{R}}$.

Sendo assim, como a estrutura $\left(\mathbb{R}^{\mathbb{R}},+\right)$ goza da associatividade, comutatividade, existência de elemento neutro e existência de elemento simétrico a toda $f\in\mathbb{R}^{\mathbb{R}}$, então $\left(\mathbb{R}^{\mathbb{R}},+\right)$ corresponde a um grupo abeliano.

Note que a multiplicação é associativa em $\left(\mathbb{R}^{\mathbb{R}},\cdot\right)$, pois para todas $f,g,h\in\mathbb{R}^{\mathbb{R}}$ e todo $x\in\mathbb{R}$,

$$[(fg)\cdot h](x)=[(fg)(x)]h(x)=[f(x)g(x)]h(x)=f(x)[g(x)h(x)]=f(x)[(gh)(x)]=[f(gh)](x)$$

devido à associatividade da multiplicação válida em $\mathbb{R}$. Da distributividade da multiplicação em relação à adição, avaliada em $\mathbb{R}$, para todas $f,g,h\in\mathbb{R}^{\mathbb{R}}$ e todo $x\in\mathbb{R}$, segue que

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

De modo análogo, podemos verificar que $[h(f+g)](x)=(hf+hg)(x)$ para todo $x\in\mathbb{R}$. Logo, $\left(\mathbb{R}^{\mathbb{R}},+,\cdot\right)$ goza da propriedade distributiva da multiplicação em relação à adição.

Devido ao conjunto de propriedades que são verificadas em $\left(\mathbb{R}^{\mathbb{R}},+,\cdot\right)$, podemos classificá-lo como anel.

Outro exemplo importante consiste na construção de anéis a partir do produto cartesiano. Nesse caso, com base nos anéis $\left(A,+,\cdot\right)$ e $\left(B,+,\cdot\right)$, podemos identificar um anel a partir do produto cartesiano entre *A* e *B*, isto é, $A\times B$. A partir desse produto cartesiano, tomando $(x,y),(z,w)\in A\times B$, podemos definir uma adição e uma multiplicação sobre $A\times B$, respectivamente,

como segue:

$$(x,y)+(z,w)=(x+z,y+w)$$

$$(x,y)\cdot(z,w)=(xz,yw)$$

Tomando o conjunto $A\times B$ munido dessas operações, a estrutura $\left(A\times B,+,\cdot\right)$ pode ser classificada como um anel caracterizado como o **produto direto** dos anéis $\left(A,+,\cdot\right)$ e $\left(B,+,\cdot\right)$. Verifique que essa estrutura goza de todas as propriedades presentes na definição de anel, tomando por base as propriedades presentes nos anéis $\left(A,+,\cdot\right)$ e $\left(B,+,\cdot\right)$.

Um terceiro exemplo importante de anel é $\left(\mathbb{Z},+,\cdot\right)$, ou seja, o anel dos inteiros, considerando as operações de adição e multiplicação usuais definidas sobre esse conjunto numérico. Quando analisamos a operação de multiplicação definida sobre o conjunto de números

inteiros, podemos observar que ela aproveita outras propriedades, além do fechamento e da associatividade. Por isso, podemos estudar não só a definição, mas também outras categorias específicas de anéis, as quais estão relacionadas com propriedades adicionais que podem ser verificadas a partir do estudo da segunda operação definida sobre o conjunto não vazio. Dentre essas, podemos destacar os anéis comutativos e os anéis com unidade.

Anel comutativo

Quando analisamos um anel $(A,+,\cdot)$, temos que a estrutura $(A,+)$ pode ser classificada como um grupo abeliano, a qual goza da propriedade comutativa, além de outras. No entanto, podemos investigar estruturas em que a segunda operação $(\cdot)$ também apresenta essa mesma propriedade, o que nos conduz ao estudo dos anéis comutativos.

Dizemos que um anel $(A,+,\cdot)$ corresponde a um **anel comutativo** quando, além de $(A,+,\cdot)$ desfrutar de todas as propriedades presentes na definição de anel, também possuir a propriedade comutativa para a operação $\cdot$, isto é, dados $x,y \in A$, então $x \cdot y = y \cdot x$.

Como principais exemplos de anéis comutativos temos $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ e $(\mathbb{C},+,\cdot)$, munidos das operações usuais de adição e multiplicação correspondentes. Isso ocorre devido a essas estruturas comporem anéis além de as multiplicações respectivas usufruírem da propriedade comutativa.

Exemplificando

O anel $(\mathbb{R}^{\mathbb{R}},+,\cdot)$ pode ser classificado como um anel comutativo. De fato, sejam $f,g \in \mathbb{R}^{\mathbb{R}}$, de modo que ao considerar $x \in \mathbb{R}$ qualquer, é possível verificar que $(f \cdot g)(x) = f(x)g(x) = g(x)f(x) = (g \cdot f)(x)$. A primeira e a última igualdades são garantidas pela definição da multiplicação de funções, enquanto a segunda é válida pela comutatividade dos números reais na multiplicação, pois $f(x),\ g(x) \in \mathbb{R}$. Portanto, $(\mathbb{R}^{\mathbb{R}},+,\cdot)$ é um anel comutativo.

Além da propriedade comutativa, a segunda operação binária de um anel $(A,+,\cdot)$ pode gozar da existência de elemento neutro, o que possibilita o estudo de outra categoria de anéis, os chamados anéis com unidade.

Anel com unidade

No estudo de um anel $(A,+,\cdot)$ temos que a estrutura $(A,+)$ pode ser classificada como um grupo abeliano, o que resulta em $(A,+)$ apresentar, dentre outras, a propriedade da existência de elemento neutro por se tratar de uma propriedade decorrente da definição de grupo. Porém, quando em relação à segunda operação $(\cdot)$ também for verificada essa propriedade, podemos definir os chamados anéis com unidade.

Dizemos que um anel $(A,+,\cdot)$ corresponde a um **anel com unidade** quando, além de $(A,+,\cdot)$ admitir todas as propriedades presentes na definição de anel, também gozar da existência de elemento neutro para a operação $\cdot$, isto é, existe um elemento $1_A \in A$ tal que para todo $x \in A$ for possível verificar que $x \cdot 1_A = 1_A \cdot x = x$. Neste caso, podemos dizer que 1_A é a **unidade** do anel $(A,+,\cdot)$. E quando for possível, podemos representar a unidade de A apenas por 1, desde que não exista a possibilidade de confusão.

Os anéis $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ e $(\mathbb{C},+,\cdot)$ admitem o número 1 como a unidade da multiplicação, implicando na classificação deles como anéis com unidade.

Exemplificando

Considere o anel $(\mathbb{R}^{\mathbb{R}},+,\cdot)$ relativo às funções reais. Esse anel pode ser classificado como um anel com unidade. Dessa forma, considerando a função constante $u:\mathbb{R}\to\mathbb{R}$ definida por $u(x)=1$ para todo $x \in \mathbb{R}$, a qual pertence ao conjunto $\mathbb{R}^{\mathbb{R}}$, teremos, para qualquer $f \in \mathbb{R}^{\mathbb{R}}$ e qualquer $x \in \mathbb{R}$,

$$(f \cdot u)(x) = f(x)u(x) = f(x) \cdot 1 = f(x)$$

$$(u \cdot f)(x) = u(x)f(x) = 1 \cdot f(x) = f(x)$$

isto é, $f \cdot u = u \cdot f = f$. Portanto, $(\mathbb{R}^{\mathbb{R}},+,\cdot)$ é um anel com unidade, sendo a função constante igual a 1.

Reflita

Com base nos conjuntos estudados na educação básica, munidos das operações usuais de adição e multiplicação correspondentes, que exemplo podemos destacar de anel $(A,+,\cdot)$ que não pode ser classificado como anel com unidade, ou seja, um anel cuja multiplicação não goza da propriedade da existência de elemento neutro?

Além das propriedades adicionais, podemos partir de um anel $(A,+,\cdot)$ e verificar a possibilidade de definir outros anéis com base em subconjuntos não vazios de *A*, construindo uma relação semelhante à dos grupos e subgrupos, agora envolvendo o conceito de anel.

Subanel

Considere $(A,+,\cdot)$ um anel. Dizemos que a estrutura $(B,+,\cdot)$, com *B* um subconjunto não vazio de *A*, corresponde a um **subanel** de $(A,+,\cdot)$ quando forem satisfeitas as seguintes condições:

(i) *B* for fechado para ambas operações definidas em *A*, ou seja, para todos $x,y \in B$ for possível verificar que $x+y \in B$ e $x \cdot y \in B$.

(ii) $(B,+,\cdot)$ gozar das propriedades que caracterizam um anel, considerando as restrições das operações $+$ e $\cdot$ definidas em *A* sobre o subconjunto *B*.

Exemplificando

A partir do conjunto $\mathbb{R}^{\mathbb{R}}$, o qual compõe o anel $\left(\mathbb{R}^{\mathbb{R}},+,\cdot\right)$, podemos definir o subconjunto $L=\left\{f \in \mathbb{R}^{\mathbb{R}} \mid f(1)=0\right\}$.

Note que *L* é não vazio, pois, por exemplo, a função $f:\mathbb{R}\to\mathbb{R}$ definida por $f(x)=x-1$ pertence a *L*, já que $f(1)=1-1=0$. Para $f,g \in L$ temos $(f+g)(1)=f(1)+g(1)=0+0=0$ e $(fg)(1)=f(1)g(1)=0\cdot 0=0$, o que implica $f+g,\ fg \in L$, comprovando a validade da condição (i) da definição de subanel e o fechamento das operações de adição e multiplicação de funções em *L*.

Veja que a estrutura $(L,+,\cdot)$ é um anel. De fato, $(L,+)$ é um grupo abeliano, pois as propriedades associativa e comutativa são verificadas

em $(L,+)$ porque são propriedades válidas em todo o conjunto $\mathbb{R}^{\mathbb{R}}$ e, em particular, no subconjunto *L* o elemento neutro de $(L,+)$ é a função nula $0 \in \mathbb{R}^{\mathbb{R}}$, a qual pertence a *L*, pois $0(x)=0$ para todo $x \in \mathbb{R}$ e, em particular, para $1 \in \mathbb{R}$. A cada função $f \in L$ veja que $-f \in L$, pois f é tal que $(-f)(x)=-f(x)$ para todo $x \in \mathbb{R}$, assim, $(-f)(1)=-f(1)=-0=0$. Ainda, $(L,+,\cdot)$ goza das propriedades associativa da multiplicação e distributiva da multiplicação em relação à adição por se tratarem de propriedades válidas em todo o $\mathbb{R}^{\mathbb{R}}$ e, em particular, em seu subconjunto *L*, comprovando a condição (ii) da definição de subanel. Portanto, podemos concluir que $(L,+,\cdot)$ é um subanel de $\left(\mathbb{R}^{\mathbb{R}},+,\cdot\right)$.

Além da definição, podemos investigar quando um subconjunto compõe um subanel de outro anel $(A,+,\cdot)$, considerando as restrições das operações ao subconjunto, a partir da seguinte proposição.

Proposição 1: considere $(A,+,\cdot)$ um anel e *B* um subconjunto não vazio de *A*. Temos que $(B,+,\cdot)$ é um subanel de $(A,+,\cdot)$ se, e somente se, para todos $x,y \in B$ for possível verificar que $x-y \in B$ e $x \cdot y \in B$, em que $x-y=x+(-y)$.

Demonstração: Suponha que $(B,+,\cdot)$ é subanel de $(A,+,\cdot)$ então, consequentemente, $(B,+)$ é um subgrupo de $(A,+)$, o que implica, para todos $x,y \in B$, $x-y \in B$. Além disso, sendo $(B,+,\cdot)$ subanel de $(A,+,\cdot)$, a operação $\cdot$ é fechada em *B*, da qual segue que $x \cdot y \in B$, comprovando a primeira condicional presente na proposição.

Por outro lado, para a segunda condicional, suponha que para todos $x,y \in B$ podemos verificar que $x-y \in B$ e $x \cdot y \in B$. Da hipótese $x-y \in B$, o que equivale a dizer $x+(-y) \in B$, para todos $a,b \in B$, segue que a operação $+$ é fechada em *B* e todo $y \in B$ admite um oposto $-y \in B$. Logo, $(B,+)$ é um subgrupo de $(A,+)$, além disso, $(B,+)$ é, em particular, um grupo abeliano devido às propriedades que decorrem do grupo abeliano $(A,+)$ e devido a $(A,+,\cdot)$ps>> ser um anel por hipótese. Pelo fechamento da operação $\cdot$, decorrente da implicação $x,y \in B$ então $x \cdot y \in B$, a estrutura $(B,+,\cdot)$ também gozará das propriedades associativa de $\cdot$ e distributiva da operação $\cdot$ em relação à $+$, por

se tratarem de propriedades válidas a todos os elementos de A e, em particular, aos elementos de seu subconjunto não vazio B. Portanto, $(B,+,\cdot)$ é um subanel de $(A,+,\cdot)$, o que conclui a segunda condicional e, consequentemente, finaliza a demonstração.

Assimile

Conforme a proposição anterior, para provar que $(B,+,\cdot)$ é um subanel de $(A,+,\cdot)$, basta comprovar que para todos $x,y \in B$ são válidas as relações de inclusão: $x-y \in B$ e $x \cdot y \in B$.

Considere, por exemplo, o conjunto não vazio $3\mathbb{Z}=\{...,-6,-3,\ 0,\ 3,\ 6,...\} \subset \mathbb{Z}$. Sabemos que $(\mathbb{Z},+,\cdot)$ pode ser classificado como anel. Vamos provar, pela proposição 1 que $(3\mathbb{Z},+,\cdot)$ corresponde a um subanel de $(\mathbb{Z},+,\cdot)$. De fato, sejam $x,y \in 3\mathbb{Z}$, existem $k,q \in \mathbb{Z}$, tais que $x=3k$ e $y=3q$. Note que $-y=-3q=3(-q)$ e $-q \in \mathbb{Z}$, logo, $-y \in 3\mathbb{Z}$. Dessa forma,

$$x-y=3k-3q=3(k-q) \quad \text{e} \quad x \cdot y=(3k)\cdot(3q)=3(3kq)$$

onde $k-q,\ 3kq \in \mathbb{Z}$. Logo, $x-y,\ x \cdot y \in 3\mathbb{Z}$. Portanto, pela proposição 1, podemos concluir que $(3\mathbb{Z},+,\cdot)$ é um subanel de $(\mathbb{Z},+,\cdot)$.

Faça você mesmo

Identifique um exemplo de conjunto não vazio $A \subset \mathbb{Z}$ tal que $(A,+,\cdot)$ não possa ser classificado como subanel de $(\mathbb{Z},+,\cdot)$.

Considere $(A,+,\cdot)$ um anel com unidade e seu subanel $(B,+,\cdot)$. Nesse caso, podemos nos deparar com as seguintes situações:

- $(A,+,\cdot)$ e $(B,+,\cdot)$ podem admitir a mesma unidade, fato que ocorre com o anel $(\mathbb{Q},+,\cdot)$ e seu subanel $(\mathbb{Z},+,\cdot)$, por exemplo.
- $(A,+,\cdot)$ admite unidade enquanto $(B,+,\cdot)$ não goza da propriedade da existência de elemento neutro para a operação $\cdot$, situação observada quando estudamos o anel $(\mathbb{Z},+,\cdot)$ e seu subanel $(2\mathbb{Z},+,\cdot)$, por exemplo.
- $(A,+,\cdot)$ e $(B,+,\cdot)$ admitem unidades diferentes, como é o caso do anel $(M_2(\mathbb{R}),+,\cdot)$ e seu subanel $(K,+,\cdot)$ com $K=\left\{A \in M_2(\mathbb{R}) \;\middle|\; A=\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}, a \in \mathbb{R}\right\}$,

porque $(M_2(\mathbb{R}),+,\cdot)$ admite a unidade $I_2=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$, enquanto a unidade de $(K,+,\cdot)$ é $u=\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}$, por exemplo.

Podemos ainda identificar casos em que o anel $(A,+,\cdot)$ e seu subanel $(B,+,\cdot)$ não admitem unidade, como quando comparamos $(2\mathbb{Z},+,\cdot)$ e seu subanel $(4\mathbb{Z},+,\cdot)$, por exemplo, e casos em que o anel $(A,+,\cdot)$ não possui unidade e seu subanel $(B,+,\cdot)$ goza dessa propriedade, como a situação do anel $(2\mathbb{Z}\times\mathbb{Z},+,\cdot)$, que não admite unidade e seu subanel $(\{0\}\times\mathbb{Z},+,\cdot)$, que possui o par $(0,1)$ como unidade.

Quando tivermos um anel $(A,+,\cdot)$ e seu subanel $(B,+,\cdot)$ de modo que ambos admitam a mesma unidade, isto é, $1_A=1_B$, podemos dizer que $(B,+,\cdot)$ é um **subanel unitário** de $(A,+,\cdot)$.

Faça você mesmo

Mostre que a estrutura $(\{0\}\times\mathbb{Z},+,\cdot)$ pode ser classificada como um anel comutativo e com unidade munido das operações definidas anteriormente no estudo do produto direto.

O estudo dos anéis e suas subcategorias, bem como dos subanéis, nos auxilia a observar quais propriedades são satisfeitas nas estruturas em estudo, possibilitando a articulação entre elas para a resolução de problemas.

Pesquise mais

Para complementar os estudos a respeito da estrutura de anel, consulte as seções 1.5 e 1.6 do livro *Estruturas Algébricas* disponível em sua biblioteca virtual.

COCHMANSKI, Julio Cesar; COCHMANSKI, Liliane Cristina de Camargo. **Estruturas algébricas**. Curitiba: InterSaberes, 2016.

Sem medo de errar

Na preparação da segunda etapa do curso de capacitação proposto aos funcionários da empresa, você deve organizar as tarefas que serão desenvolvidas, resolvendo-as e apresentando comentários de modo a construir um roteiro que possa auxiliá-lo durante a aplicação da capacitação.

Nesta etapa do curso, o objetivo é que os funcionários estudem as propriedades das matrizes quadradas de ordem 2 com entradas reais, munido das operações usuais de adição e multiplicação de matrizes, compondo a estrutura $(M_2(\mathbb{R}),+,\cdot)$.

A primeira questão consiste verificar que $(M_2(\mathbb{R}),+,\cdot)$ é um anel. Note que $(M_2(\mathbb{R}),+)$ é um grupo abeliano. De fato, o fechamento é satisfeito em $(M_2(\mathbb{R}),+)$ porque a soma de matrizes quadradas de ordem 2 com entradas reais resulta em uma matriz desse mesmo tipo e, considerando matrizes $A,B,C \in M_2(\mathbb{R})$ quaisquer, a propriedade associativa é satisfeita, pois $A+(B+C)=(A+B)+C$, bem como a comutativa, porque $A+B=B+A$. O elemento neutro da adição de matrizes é a matriz nula de ordem 2, a qual tem todas as entradas nulas e pode ser denotada por $0=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$. A existência de elemento simétrico é satisfeita a toda matriz de $M_2(\mathbb{R})$, pois se $A=(a_{ij}) \in M_2(\mathbb{R})$, podemos identificar que $-A=(-a_{ij}) \in M_2(\mathbb{R})$, de modo que $A+(-A)=(a_{ij}+(-a_{ij}))=0$. A multiplicação em $(M_2(\mathbb{R}),+,\cdot)$ é associativa, pois para todos $A,B,C \in M_2(\mathbb{R})$, é válida a relação $A(BC)=(AB)C$. Além disso, a distributividade da multiplicação em relação à adição é válida, visto que $A(B+C)=AB+AC$ e $(B+C)A=BA+CA$ para todos $A,B,C \in M_2(\mathbb{R})$. Dessa forma, podemos concluir que $(M_2(\mathbb{R}),+,\cdot)$ é um anel.

Note que $(M_2(\mathbb{R}),+,\cdot)$ não pode ser classificado como anel comutativo. De fato, tomando as matrizes $A=\begin{bmatrix}1 & -1\\ 0 & 2\end{bmatrix}, B=\begin{bmatrix}2 & -1\\ -1 & 0\end{bmatrix} \in M_2(\mathbb{R})$, podemos observar que

$$AB=\begin{bmatrix}1 & -1\\ 0 & 2\end{bmatrix}\begin{bmatrix}2 & -1\\ -1 & 0\end{bmatrix}=\begin{bmatrix}3 & -1\\ -2 & 0\end{bmatrix} \quad \text{e} \quad BA=\begin{bmatrix}2 & -1\\ -1 & 0\end{bmatrix}\begin{bmatrix}1 & -1\\ 0 & 2\end{bmatrix}=\begin{bmatrix}2 & -4\\ -1 & 1\end{bmatrix}$$

Logo, $AB \neq BA$, fazendo com que a multiplicação de matrizes não seja comutativa, indicando que o anel $(M_2(\mathbb{R}),+,\cdot)$ não é comutativo. Por outro lado, $(M_2(\mathbb{R}),+,\cdot)$ pode ser classificado como anel com unidade, pois da matriz identidade $I_2=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \in M_2(\mathbb{R})$ temos, para toda $A=\begin{bmatrix}x & y\\ z & w\end{bmatrix} \in M_2(\mathbb{R})$:

$$AI_2=\begin{bmatrix}x & y\\ z & w\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}=\begin{bmatrix}x & y\\ z & w\end{bmatrix}=A \quad \text{e} \quad I_2A=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}x & y\\ z & w\end{bmatrix}=\begin{bmatrix}x & y\\ z & w\end{bmatrix}=A$$

isto é, $AI_2=I_2A=A$, sendo I_2 o elemento neutro da multiplicação de matrizes. Dessa forma, $(M_2(\mathbb{R}),+,\cdot)$ é um anel com unidade.

Como segunda parte de sua tarefa é necessário elaborar uma atividade que envolva o conceito de subanel e o anel $(M_2(\mathbb{R}),+,\cdot)$. Uma proposta de tarefa é identificar, a partir do

anel $(M_2(\mathbb{R}),+,\cdot)$ um exemplo de subanel que não contenha unidade, ou seja, um subanel que não satisfaça a propriedade da existência de elemento neutro para a multiplicação de matrizes.

Considere a estrutura $(T,+,\cdot)$, tal que $T=\left\{A\in M_2(\mathbb{R}) \;\middle|\; A=\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}, a,b,c\in\mathbb{R}\right\}$.

Veja que $(T,+,\cdot)$ é um subanel de $(M_2(\mathbb{R}),+,\cdot)$, pois, tomando $X=\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}, Y=\begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}\in T$, temos

$$X-Y=\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}-\begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}=\begin{bmatrix} a-c & 0 \\ b-d & 0 \end{bmatrix}\in T$$

$$XY=\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}\begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}=\begin{bmatrix} ac & 0 \\ bc & 0 \end{bmatrix}\in T$$

porque $a-c,\ b-d,\ ac,\ bc\in\mathbb{R}$. Logo, pela proposição 1, podemos concluir que $(T,+,\cdot)$ é subanel de $(M_2(\mathbb{R}),+,\cdot)$. Agora, considere $x=\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}\in T$ uma matriz qualquer. Não é possível identificar uma única matriz $U=\begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix}\in T$ tal que $XU=UX=X$ porque, para isso, devemos ter

$$XU=\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}\begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix}=\begin{bmatrix} ax & 0 \\ bx & 0 \end{bmatrix}=\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}=X$$

$$UX=\begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix}\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}=\begin{bmatrix} ax & 0 \\ ay & 0 \end{bmatrix}=\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}=X$$

assim, o seguinte sistema deverá ser válido:

$$\begin{cases} ax=a \\ bx=b \\ ay=b \end{cases}$$

Para isso, devemos ter $x=1$ e $y=b/a$, com $a\neq 0$, no entanto, essa expressão não poderá ser válida porque $a,b\in\mathbb{R}$ são quaisquer, implicando em *y* ser variável e, assim, a matriz *U* não pode ser única. Portanto, o anel $(T,+,\cdot)$ não goza da propriedade da existência de elemento neutro para a multiplicação.

Para finalizar, organize em um documento as tarefas que deverão ser executadas pelos funcionários na segunda etapa

do curso, da forma como elas deverão ser apresentadas a eles (material impresso, apresentação de slides, etc.), organizando também um documento com todas as atividades resolvidas, indicando possíveis dúvidas e encaminhamentos que podem ser adotados frente a essas dúvidas. Procure destacar, em cada etapa, os conhecimentos necessários e a importância da definição de anel para o desenvolvimento das tarefas propostas.

Avançando na prática

Os conceitos de anéis e subanéis associados ao estudo do plano e espaço cartesianos

Descrição da situação-problema

Suponha que você seja um professor e esteja elaborando um plano de aula voltado ao estudo das características do espaço cartesiano com o auxílio de softwares, como o GeoGebra (software gratuito disponível em: <https://www.geogebra.org/?lang=pt>. Acesso em: 10 ago. 2018). Para esse trabalho, você está considerando como conhecimento prévio o estudo do plano cartesiano e suas propriedades. O espaço cartesiano pode ser interpretado como a representação geométrica do espaço $\mathbb{R}^3$, composto pelas ternas ordenadas (x,y,z) de números reais, enquanto o plano cartesiano consiste na representação geométrica do espaço $\mathbb{R}^2$, composto pelos pares ordenados (x,y) de números reais. Em muitos trabalhos, estudamos o plano coordenado xy do espaço cartesiano de modo análogo ao plano cartesiano $\mathbb{R}^2$, devido a possibilidade de interpretar xy como o conjunto das ternas $(x,y,0)$, com $x,y \in \mathbb{R}$. Por esta razão, podemos associar esses espaços entre si por meio da relação de inclusão de conjuntos. Considerando a definição de operações de adição e multiplicação sobre $\mathbb{R}^3$ semelhantes à do produto direto (como soma e multiplicação coordenada a coordenada), podemos compor o anel $(\mathbb{R}^3,+,\cdot)$. Com base nessas informações, justifique que <<Eqn329.eps>> é um subanel de $(\mathbb{R}^3,+,\cdot)$, com $A=\{(x,y,0)\,|\,x,y \in \mathbb{R}\}$. Finalize os estudos com a elaboração de uma tarefa que possibilite a associação do plano coordenado xy com o espaço $\mathbb{R}^3$ utilizando *softwares* e

empregando as propriedades analisadas, interpretando as ternas (x, y, z) como vetores no espaço $\mathbb{R}^3$.

Resolução da situação-problema

Sobre o espaço $\mathbb{R}^3 = \{(x, y, z) | x, y, z \in \mathbb{R}\}$ podemos definir a adição e a multiplicação de modo que, para todos $x = (x_1, x_2, x_3), y = (y_1, y_2, y_3) \in \mathbb{R}^3$, $x + y = (x_1 + y_1, x_2 + y_2, x_3 + y_3)$ e $xy = (x_1 y_1, x_2 y_2, x_3 y_3)$.

Se $x = (x_1, x_2, 0), y = (y_1, y_2, 0) \in A$ temos $x - y = (x_1, x_2, 0) - (y_1, y_2, 0) = (x_1 - y_1, x_2 - y_2, 0) \in A$ e $xy = (x_1, x_2, 0) \cdot (y_1, y_2, 0) = (x_1 y_1, x_2 y_2, 0) \in A$. Sendo assim, como $x - y, xy \in A$ para todos $x, y \in A$, podemos concluir que $(A, +, \cdot)$ é um subanel de $(\mathbb{R}^3, +, \cdot)$.

Para a elaboração da tarefa, podem ser propostas atividades que seja necessário somar vetores na forma $x = (x_1, x_2, 0) \in A$, pertencentes ao plano coordenado xy, explorando a comutatividade, a associatividade, bem como as demais propriedades, observando que a operação aplicada entre vetores desse plano sempre resultará em um vetor desse mesmo plano coordenado, sendo esta uma consequência do fechamento de ambas as operações definidas sobre $\mathbb{R}^3$ e restritas ao conjunto *A*.

Faça valer a pena

1. Considere o anel dos racionais, ou seja, o anel comutativo e com unidade descrito por $(\mathbb{Q}, +, \cdot)$ e o subconjunto dos racionais definido por $S = \{x \in \mathbb{Q} | x \notin \mathbb{Z}\}$.

Com base nos conjuntos apresentados, munidos das operações usuais de adição e multiplicação de racionais, analise as seguintes afirmativas e a relação proposta entre elas:

I. A estrutura $(S, +, \cdot)$ pode ser classificada como subanel de $(\mathbb{Q}, +, \cdot)$.

PORQUE

II. A operação de multiplicação restrita a *S* não goza da propriedade comutativa.

Em relação às afirmativas apresentadas, assinale a alternativa correta:

a) As afirmativas I e II estão corretas, e a II é uma justificativa correta para a I.
b) As afirmativas I e II estão corretas, mas a II não é uma justificativa correta para a I.

c) A afirmativa I está correta e a II está incorreta.
d) A afirmativa II está correta e a I está incorreta.
e) As afirmativas I e II estão incorretas.

2. As classificações das estruturas compostas por conjuntos não vazios, munidos de duas operações binárias correspondentes, como anéis está diretamente relacionada às propriedades que podem ser verificadas em função dos elementos presentes nos conjuntos em estudo.
Com base nesse tema, considere as estruturas descritas a seguir:

- $A = M_3(\mathbb{R})$, munido das operações usuais de adição e multiplicação de matrizes, compondo a estrutura $(A, +, \cdot)$
- $B = 4\mathbb{Z}$, munido das operações usuais de adição e multiplicação de números inteiros, compondo a estrutura $(B, +, \cdot)$
- $C = \mathbb{N}$, munido das operações usuais de adição e multiplicação de números naturais, compondo a estrutura $(C, +, \cdot)$
- $D = \mathbb{R} \times \mathbb{R} = \mathbb{R}^2$, munido das operações usuais de adição e multiplicação, decorrentes do produto direto, compondo a estrutura $(D, +, \cdot)$

Além disso, considere as seguintes categorias:

- I – anel comutativo sem unidade
- II – anel comutativo com unidade
- III – não é anel
- IV – anel não comutativo com unidade

Considerando as estruturas e as categorias apresentadas, assinale a alternativa que indica todas as associações corretamente.

a) I – $(A, +, \cdot)$; II – $(C, +, \cdot)$; III – $(B, +, \cdot)$; IV – $(D, +, \cdot)$.
b) I – $(B, +, \cdot)$; II – $(D, +, \cdot)$; III – $(C, +, \cdot)$; IV – $(A, +, \cdot)$.
c) I – $(C, +, \cdot)$; II – $(A, +, \cdot)$; III – $(B, +, \cdot)$; IV – $(D, +, \cdot)$.
d) I – $(D, +, \cdot)$; II – $(A, +, \cdot)$; III – $(C, +, \cdot)$; IV – $(B, +, \cdot)$.
e) I – $(D, +, \cdot)$; II – $(B, +, \cdot)$; III – $(A, +, \cdot)$; IV – $(C, +, \cdot)$.

3. Considere o conjunto $P = \{a, b, c, d\}$ e suponha que $(P, +, \cdot)$ corresponda a um anel com unidade que apresenta as seguintes características:

- O elemento neutro de $(P, +, \cdot)$ referente à operação $+$ é *a*.
- O elemento neutro de $(P, +, \cdot)$ referente à operação $\cdot$ é *b*.
- As seguintes igualdades são válidas: $b + b = a$, $c + c = a$ e $c \cdot d = a$.

Com base nessas informações, um estudante construiu as tábuas indicadas na Figura 3.1.

Figura 3.1 | Tábuas de $(P, +, \cdot)$

$+$	a	b	C	d
a	a	b	I	d
b	b	a	d	c
c	III	d	a	b
d	d	c	b	II

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	c	V
d	a	IV	a	d

Fonte: elaborada pela autora.

Com base nas informações apresentadas, assinale a alternativa que indica quais elementos devem compor as posições I, II, III, IV e V das tábuas apresentadas na Figura 3.1.

a) I – *d*; II – *b*; III – *c*; IV – *c*; V – *a*.
b) I – *a*; II – *a*; III – *b*; IV – *d*; V – *c*.
c) I – *c*; II – *d*; III – *a*; IV – *b*; V – *b*.
d) I – *d*; II – *c*; III – *d*; IV – *a*; V – *d*.
e) I – *c*; II – *a*; III – *c*; IV – *d*; V – *a*.

Seção 3.3

Anéis de integridade

Diálogo aberto

Nas seções anteriores estudamos os anéis e suas principais categorias, como os anéis comutativos e os anéis com unidade. Neste estudo, com base em um conjunto não vazio munido de duas operações binárias, analisamos que propriedades deveriam estar associadas a cada classificação, além de alguns exemplos importantes. Nesta seção, prosseguiremos com o estudo dos anéis ou domínios de integridade e as relações entre as diferentes categorias de anéis.

Para isso, ainda consideraremos o contexto de atuação na empresa de tecnologia, para finalizar a preparação do curso de capacitação que será ministrado a um grupo de funcionários. Sua tarefa será a de estruturar a etapa final dessa capacitação, organizando as propostas a serem desenvolvidas pelos funcionários durante o curso, analisando os conceitos da teoria de anéis que deverão ser empregados por eles e as possíveis dificuldades que podem surgir nesse processo. Você deverá elaborar o material que será aplicado no terceiro dia do curso e um documento com orientações que possa auxiliar na condução da capacitação, além do problema a ser considerado, que já foi selecionado e é apresentado a seguir.

O algoritmo computacional de uma máquina para cortes de chapas metálicas funciona com base no estudo do conjunto dos inteiros módulo 6, representado por $\mathbb{Z}_6$. Assim, ao longo dos cálculos realizados pelo algoritmo, existe a necessidade de avaliar as divisões de números inteiros por 6 e agrupá-los de acordo com os restos obtidos nessas divisões, sendo estes restos relacionados com os desperdícios de matérias-primas associados a cada tipo de corte. Dessa forma, na etapa final do curso, os funcionários precisarão avaliar as características do conjunto $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ com suas operações usuais de adição e multiplicação. Para isso, será necessário responder às seguintes questões:

a) Demonstre que o conjunto $\mathbb{Z}_6$, com as operações usuais de adição e multiplicação, pode ser classificado como um anel comutativo com unidade.

b) Mostre que o anel $(\mathbb{Z}_6, +, \cdot)$ não pode ser classificado como um anel de integridade.

c) Existe algum tipo de conjunto na forma $\mathbb{Z}_m$, com m natural, que em conjunto com as operações usuais pode ser classificado como um anel de integridade? Cite um exemplo justificando sua resposta.

Para a elaboração do documento com orientações para aplicação da capacitação, resolva o problema proposto, identificando as justificativas e os conhecimentos associados, considerando as propriedades do conjunto dos inteiros módulo m, bem como as possíveis dúvidas e os encaminhamentos que podem ser adotados para sanar as dúvidas elencadas.

Após a realização desta tarefa, você estará apto a finalizar o plano da capacitação, organizando todas as informações construídas ao longo da unidade.

Não pode faltar

Na seção anterior verificamos que os anéis podem ser organizados em subcategorias, as quais são construídas com base em propriedades adicionais que são verificadas ao analisar a segunda operação binária definida sobre o conjunto, ou seja, as propriedades que são satisfeitas em $(A, \cdot)$ considerando o estudo do anel $(A, +, \cdot)$.

Dado um anel $(A, +, \cdot)$, quando $(A, \cdot)$ goza da propriedade comutativa, então $(A, +, \cdot)$ será um anel comutativo e se $(A, \cdot)$ goza da existência do elemento neutro, $(A, +, \cdot)$ será um anel com unidade.

Assimile

Se $(A, +, \cdot)$ é um anel, da definição podemos observar que $(A, +)$ é um grupo abeliano, o qual goza das propriedades do fechamento, associativa, comutativa, existência de elemento neutro e existência de elemento simétrico a todo elemento do conjunto. Por isso, quando investigamos se um anel é comutativo ou admite unidade precisamos analisar a estrutura

$(A,\cdot)$, ou seja, avaliar se a comutatividade e a existência de elemento neutro são satisfeitas considerando a operação $\cdot$.

Analisando os casos discutidos na seção anterior, como o exemplo de anel comutativo, podemos citar o anel $(2\mathbb{Z},+,\cdot)$, no qual, além das propriedades características da definição de anel, é satisfeita também a comutatividade da multiplicação de inteiros restrita aos inteiros múltiplos de 2. Porém, note que esse anel não goza da existência de elemento neutro para a multiplicação, porque $1 \notin 2\mathbb{Z}$ e 1 é o único número inteiro que satisfaz a relação $1 \cdot x = x \cdot 1 = x$ para todo x inteiro e, consequentemente, todo $x \in 2\mathbb{Z}$.

O anel $(M_3(\mathbb{R}),+,\cdot)$, chamado de anel das matrizes quadradas de ordem 3 com entradas reais munido da adição e multiplicação usuais de matrizes, pode ser classificado como um anel com unidade. O elemento neutro da estrutura $(M_3(\mathbb{R}),+,\cdot)$ corresponde à matriz identidade de ordem 3, que pode ser dada por $I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. Porém, observe que esse anel não pode ser classificado como anel comutativo, pois a multiplicação de matrizes em $(M_3(\mathbb{R}),+,\cdot)$ não é comutativa.

Nos exemplos citados, temos estruturas que são anéis com unidade ou anéis comutativos, de modo que em nenhum dos dois casos as duas categorias podem ser avaliadas simultaneamente. No entanto, existem estruturas que gozam, para a segunda operação binária, tanto da comutatividade como da existência de elemento neutro, compondo assim os chamados anéis comutativos com unidade.

Anéis comutativos com unidade

Um anel $(A,+,\cdot)$ cuja operação $\cdot$ goza, simultaneamente, da propriedade comutativa e da existência de elemento neutro (admite unidade) pode ser classificado como um **anel comutativo com unidade**.

Dentre os principais exemplos que temos de anéis comutativos com unidade, podemos destacar os anéis numéricos $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ e $(\mathbb{C},+,\cdot)$. Além disso, outro exemplo de anel comutativo com unidade consiste no $(\mathbb{R}^{\mathbb{R}},+,\cdot)$, o anel das funções de uma variável real munido das operações usuais de adição e multiplicação de funções, estudado com mais detalhes na seção anterior.

Vamos observar mais especificamente porque o anel $(\mathbb{C},+,\cdot)$ é comutativo com unidade.

Exemplificando

Considere o conjunto dos números complexos munido da adição e da multiplicação usuais, compondo a estrutura $(\mathbb{C},+,\cdot)$, a qual pode ser classificada como anel. Note que $(\mathbb{C},+)$ é um grupo abeliano, conforme visto na Unidade 2. Além disso, temos que a multiplicação em $\mathbb{C}$ é associativa, pois para todos $x=a+bi$, $y=c+di$ e $z=e+fi$ números complexos, pela validade da associatividade e da comutatividade de ambas as operações e a distributividade da multiplicação em relação à adição em $(\mathbb{R},+,\cdot)$, segue que

$$\begin{aligned}(x\cdot y)\cdot z &= \big[(ac-bd)+(ad+bc)i\big]\cdot(e+fi)\\ &= \big[(ac-bd)e-(ad+bc)f\big]+\big[(ac-bd)f+(ad+bc)e\big]i\\ &= \big[(ace-bde)+(-adf-bcf)\big]+\big[(acf-bdf)+(ade+bce)\big]i\\ &= \big[a(ce-df)-b(de+cf)\big]+\big[a(cf+de)+b(-df+ce)\big]i\\ &= \big[a(ce-df)-b(cf+de)\big]+\big[a(cf+de)+b(ce-df)\big]i\\ &= (a+bi)\cdot\big[(ce-df)+(cf+de)i\big]=x\cdot(y\cdot z)\end{aligned}$$

A propriedade distributiva da multiplicação em relação à adição é também válida em $(\mathbb{C},+,\cdot)$, pois para todos $x=a+bi$, $y=c+di$ e $z=e+fi$ números complexos, sendo válidas a associatividade e a comutatividade de ambas as operações, bem como a distributividade da multiplicação em relação à adição em $(\mathbb{R},+,\cdot)$, temos que

$$\begin{aligned}(x+y)\cdot z &= \big[(a+c)+(b+d)i\big]\cdot(e+fi)\\ &= \big[(a+c)e-(b+d)f\big]+\big[(a+c)f+(b+d)e\big]i\\ &= \big[(ae+ce)-(bf+df)\big]+\big[(af+cf)+(be+de)\big]i\\ &= (ae+ce)-(bf+df)+(af+cf)i+(be+de)i\\ &= \big[(ae-bf)+(af+be)i\big]+\big[(ce-df)+(cf+de)i\big]\\ &= \big[(a+bi)(e+fi)\big]+\big[(c+di)(e+fi)\big]\\ &= x\cdot z+y\cdot z\end{aligned}$$

De modo análogo, podemos verificar que $x \cdot (y + z) = x \cdot y + x \cdot z$. Portanto, $(\mathbb{C}, +, \cdot)$ é um anel.

A multiplicação em $(\mathbb{C}, +, \cdot)$ é comutativa, pois para todos $x = a + bi$ e $y = c + di$ números complexos, segue que

$$x \cdot y = (a + bi)(c + di) = (ac - bd) + (ad + bc)i$$
$$= (ca - db) + (da + cb)i = (c + di)(a + bi) = y \cdot x$$

Além disso, a multiplicação de números complexos goza da propriedade de existência de elemento neutro, pois tomando $1 = 1 + 0i \in \mathbb{C}$, podemos verificar que

$$x \cdot 1 = (a + bi)(1 + 0i) = (a \cdot 1 - b \cdot 0) + (a \cdot 0 + b \cdot 1)i = a + bi = x$$

$$1 \cdot x = (1 + 0i)(a + bi) = (1 \cdot a - 0 \cdot b) + (0 \cdot a + 1 \cdot b)i = a + bi = x$$

Isto é, $x \cdot 1 = 1 \cdot x = x$ para todo $x = a + bi \in \mathbb{C}$. Dessa forma, $1 = 1 + 0i \in \mathbb{C}$ corresponde à unidade da multiplicação de complexos.

Portanto, $(\mathbb{C}, +, \cdot)$ pode ser classificado como anel comutativo com unidade.

Sendo assim, para que um anel $(A, +, \cdot)$ seja classificado como anel comutativo com unidade, é necessário que a estrutura $(A, \cdot)$ goze das propriedades comutativa e da existência de elemento neutro, além das propriedades associativa e do fechamento, que são parte da definição de anel.

Faça você mesmo

Identifique um exemplo de anel comutativo com unidade que envolva um conjunto diferente dos conjuntos numéricos e estude suas propriedades.

O anel dos inteiros $(\mathbb{Z}, +, \cdot)$ pode também ser classificado como anel comutativo com unidade, basta verificar que, além de satisfazer as propriedades de anel, a multiplicação de inteiros goza

da comutatividade e da existência de elemento neutro, sendo o número 1 sua unidade.

Quando resolvemos equações com base no anel $(\mathbb{Z},+,\cdot)$ e nos deparamos com expressões da forma $3x=0$, por exemplo, podemos concluir que $x=0$, ou seja, que a equação $3x=0$ admite a solução $x=0$. Mas como podemos fundamentar essa afirmação? Esse tipo de estudo é possível porque $(\mathbb{Z},+,\cdot)$ pode ser classificado como um anel ou domínio de integridade, estrutura que estudaremos na sequência.

Anéis ou domínios de integridade

Considere um anel $(A,+,\cdot)$. Se $(A,+,\cdot)$ for um anel comutativo com unidade, com o elemento neutro da operação $+$ representado por e_A, e, além disso, gozar da seguinte propriedade:

(i) Se $a,b\in A$ e $a\cdot b=e_A$, então $a=e_A$ ou $b=e_A$,

dizemos que $(A,+,\cdot)$ é um **anel** ou **domínio de integridade**. Quando não houver possibilidade de confusão, podemos adotar as notações e, 0_A ou 0 para o elemento neutro de $+$.

Assimile

A propriedade "Se $a,b\in A$ e $a\cdot b=e_A$, então $a=e_A$ ou $b=e_A$ pode ser chamada de lei do anulamento do produto. Analisando a contrapositiva dessa lei teremos a seguinte propriedade em $(A,+,\cdot)$: "Se $a\neq e_A$ e $b\neq e_A$, então $a\cdot b\neq e_A$". Assim, podemos avaliar a lei do anulamento do produto a partir de sua forma original ou por sua contrapositiva, sendo ambas equivalentes.

Considerando novamente o anel $(\mathbb{Z},+,\cdot)$, que pode ser classificado como anel comutativo com unidade, quando tomamos dois números inteiros *a* e *b* não nulos, temos que o produto *ab* será também não nulo (ou seja, diferente do elemento neutro da operação $+$), o que evidencia a validade da lei do anulamento do produto em $(\mathbb{Z},+,\cdot)$. Logo, devido a essas condições, podemos concluir que $(\mathbb{Z},+,\cdot)$ é um domínio de integridade. Além desse exemplo, os anéis numéricos $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ e $(\mathbb{C},+,\cdot)$ podem ser classificados como domínios de integridade. Por isso, em qualquer um desses conjuntos, se tivermos dois números diferentes de zero, o produto entre eles será também um número não nulo.

Reflita

Por que o anel $\left(\mathbb{R}^{\mathbb{R}}, +, \cdot\right)$ das funções de uma variável real, munido das operações usuais de adição e multiplicação de funções, não pode ser classificado como um domínio de integridade?

Para averiguar se um anel pode ser classificado como domínio de integridade, precisamos verificar três condições: se o anel é comutativo, se o anel admite unidade e se a lei do anulamento do produto é satisfeita. Caso uma dessas condições não seja verificada, podemos concluir que o anel em questão não é um domínio de integridade. Por exemplo, esse é o caso do anel $\left(M_3(\mathbb{R}), +, \cdot\right)$, o qual não pode ser classificado como um domínio de integridade por não ser um anel comutativo. Além disso, o anel $\left(M_3(\mathbb{R}), +, \cdot\right)$ admite os chamados divisores de zero.

Considere um anel $\left(A, +, \cdot\right)$ e $a \in A$, $a \neq e_A$. Dizemos que a é um **divisor de zero** quando existir um elemento $b \in A$, com $b \neq e_A$, tal que $a \cdot b = e_A$, com e_A elemento neutro da operação $+$.

Note que no anel $\left(M_3(\mathbb{R}), +, \cdot\right)$, tomando as matrizes não nulas *A* e *B* dadas por

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad e \quad B = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ -1 & 0 & 1 \end{bmatrix}$$

observamos que $AB = 0$. Logo, podemos concluir que *A* e *B* são divisores de zero no anel de matrizes $\left(M_3(\mathbb{R}), +, \cdot\right)$. Assim, no anel $\left(M_3(\mathbb{R}), +, \cdot\right)$ temos que a lei do anulamento do produto não é satisfeita, confirmando novamente que $\left(M_3(\mathbb{R}), +, \cdot\right)$ não é um domínio de integridade.

Como consequência da lei do anulamento do produto temos a seguinte propriedade:

Propriedade 7: Sejam $\left(A, +, \cdot\right)$ um domínio de integridade e $a, b, c \in A$. Se é válida a igualdade $a \cdot b = a \cdot c$, com $a \neq e_A$, então podemos concluir que $b = c$.

De fato, se é válida a igualdade $a \cdot b = a \cdot c$, adicionando o elemento oposto a $a \cdot c$ em ambos os membros dessa igualdade obtemos

$$a \cdot b + (-a \cdot c) = a \cdot c + (-a \cdot c) \Rightarrow a \cdot b - a \cdot c = a \cdot c - a \cdot c \Rightarrow a \cdot b - a \cdot c = e_A$$

Pela distributividade da multiplicação em relação à adição, a última igualdade implica $a \cdot (b - c) = e_A$. Como $a \neq e_A$ e $(A, +, \cdot)$ é um domínio de integridade, ou seja, goza da lei do anulamento do produto, obtemos $b - c = e_A$. Adicionando o oposto a $-c$ em ambos os membros da última igualdade, segue que

$$(b - c) + c = e_A + c \Rightarrow b + (-c + c) = c \Rightarrow b + e_A = c \Rightarrow b = c$$

Portanto, podemos concluir que, sendo $a \neq e_A$, então $b = c$.

A propriedade 7 pode ser interpretada como a lei do cancelamento aplicada à segunda operação binária de um domínio de integridade $(A, +, \cdot)$.

As propriedades dos domínios de integridade podem ser empregadas para o estudo dos conjuntos envolvidos ou de outras estruturas que podem ser construídas a partir deles, como é o caso do exemplo a seguir.

Exemplificando

Considere o anel dos inteiros $(\mathbb{Z}, +, \cdot)$, o qual corresponde a um domínio de integridade. Tomando $a \in \mathbb{Z}$, com a não nulo, vamos definir a função $f_a : \mathbb{Z} \to \mathbb{Z}$ com a lei de formação dada por $f_a(x) = ax$, para todo *x* inteiro.

Sabendo que $(\mathbb{Z}, +, \cdot)$ é um domínio de integridade, verifiquemos que a função f_a é injetiva, ou seja, dados $x, y \in \mathbb{Z}$ com $f(x) = f(y)$, então $x = y$.

Consideremos $x, y \in \mathbb{Z}$ com $f(x) = f(y)$, sendo assim, $ax = ay$. Como $a \neq 0$ e $(\mathbb{Z}, +, \cdot)$ é um domínio de integridade, pela lei do cancelamento podemos concluir que $x = y$, o que comprova a injetividade da função f_a.

Relações entre as categorias de anéis

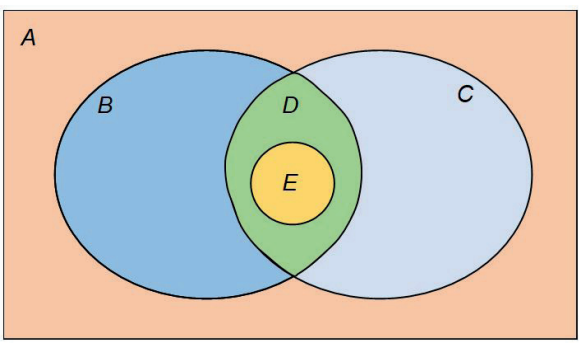
Ao longo da unidade estudamos a definição de anel e suas principais subcategorias, como os anéis comutativos, com unidade e domínios de integridade. Podemos relacionar essas categorias entre si com base nas propriedades características.

Temos que anel corresponde à categoria mais geral, a qual abrange todas as demais. A partir dela podemos observar que:

- Um anel comutativo corresponde a um anel no qual a segunda operação binária goza da comutatividade, então corresponde a um caso particular de anel.
- Um anel com unidade corresponde a um anel no qual a segunda operação binária goza da propriedade da existência de elemento neutro, então corresponde a um outro caso particular de anel.
- Um anel comutativo com unidade corresponde a um anel no qual a segunda operação binária goza da comutatividade e da propriedade da existência de elemento neutro simultaneamente, então corresponde a um caso particular de anel e, mais especificamente, a um caso particular tanto dos anéis comutativos como dos anéis com unidade, portanto, corresponde à interseção entre as categorias anel comutativo e anel com unidade.
- Um domínio de integridade corresponde a um anel comutativo com unidade que goza da lei do anulamento do produto, então corresponde a um caso particular de anel comutativo com unidade.

Podemos representar essas associações por meio de um diagrama, conforme apresentado na Figura 3.2. Nela, consideramos *A* como o conjunto dos anéis, *B* o conjunto dos anéis comutativos, *C* o conjunto dos anéis com unidade, *D* o conjunto dos anéis comutativos com unidade e *E* o conjunto dos domínios de integridade.

Figura 3.2 | Relações entre tipos de anéis



Fonte: elaborada pela autora.

A partir dessas relações podemos construir afirmações na forma:

- Todo domínio de integridade é um anel comutativo.
- Todo domínio de integridade é um anel com unidade.

Reflita

Que outras relações podem ser construídas a partir do diagrama apresentado na Figura 3.2, considerando os anéis e suas subcategorias?

Pesquise mais

Para complementar os estudos a respeito dos domínios de integridade e das demais categorias de anéis, consulte o capítulo 3 do trabalho de conclusão de curso intitulado *Uma introdução ao estudo de anéis e corpos*. Disponível em: <https://www.lume.ufrgs.br/bitstream/handle/10183/133730/000986211.pdf?sequence=1>. Acesso em: 10 ago. 2018.

Consulte também o material intitulado *Grupos, anéis e corpos e suas propriedades*, o qual apresenta um resumo a respeito dos grupos e anéis. Disponível em: <http://www.dca.fee.unicamp.br/~marco/cursos/ia012_14_1/slides/grupos-aneis-corpos.pdf>. Acesso em: 10 ago. 2018.

Sem medo de errar

Para a terceira etapa do curso de capacitação voltado aos funcionários, você ficou responsável por estruturar a proposta a ser desenvolvida resolvendo a tarefa, a fim de verificar se está adequada, identificando as possíveis dúvidas que podem ser manifestadas pelos funcionários durante os trabalhos e organizando um roteiro que contribua com a aplicação da tarefa.

O algoritmo a ser estudado no terceiro dia de curso está relacionado ao conjunto $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ com suas operações usuais de adição e multiplicação. O conjunto $\mathbb{Z}_6$ contém as classes de resto da divisão dos números inteiros por 6, sendo composto por:

$\bar{0} = \{..., -6, 0, 6, 12, ...\}$, $\bar{1} = \{..., -5, 1, 7, 13, ...\}$

, $\overline{2}=\{...,-4,\ 2,\ 8,\ 14,...\}$, $\overline{3}=\{...,-3,\ 3,\ 9,\ 15,...\}$, $\overline{4}=\{...,-2,\ 4,\ 10,\ 16,...\}$ e $\overline{5}=\{...,-1,\ 5,\ 11,\ 17,...\}$, os quais são subconjuntos de $\mathbb{Z}$. As operações de adição e multiplicação definidas sobre $\mathbb{Z}_6$ são tais que, dados $x,y\in\mathbb{Z}_6$, então $\overline{x}+\overline{y}=\overline{x+y}$ e $\overline{x}\cdot\overline{y}=\overline{xy}$, respectivamente.

A primeira parte da tarefa a ser executada pelos funcionários consiste em provar que $(\mathbb{Z}_6,+,\cdot)$ é um anel comutativo com unidade. Temos que $(\mathbb{Z}_6,+,\cdot)$ goza do fechamento relativo a ambas as operações. Na estrutura $(\mathbb{Z}_6,+)$ as propriedades associativa e comutativa são válidas, pois dados $x,y,z\in\mathbb{Z}_6$ são verificadas, respectivamente, as expressões

$$\overline{x}+\left(\overline{y}+\overline{z}\right)=\overline{x}+\overline{y+z}=\overline{x+(y+z)}=\overline{(x+y)+z}=\overline{x+y}+\overline{z}=\left(\overline{x}+\overline{y}\right)+\overline{z}$$

$$\overline{x}+\overline{y}=\overline{x+y}=\overline{y+x}=\overline{y}+\overline{x}$$

O elemento neutro da adição corresponde a $\overline{0}$, pois dado qualquer $\overline{x}\in\mathbb{Z}_6$, segue que $\overline{x}+\overline{0}=\overline{x+0}=\overline{x}$ e $\overline{0}+\overline{x}=\overline{0+x}=\overline{x}$. A classe $\overline{6-x}$ corresponde ao oposto de $\overline{x}\in\mathbb{Z}_6$, pois

$$\overline{x}+\overline{6-x}=\overline{x+(6-x)}=\overline{x+(-x+6)}=\overline{(x+(-x))+6}=\overline{0+6}=\overline{6}=\overline{0}$$

$$\overline{6-x}+\overline{x}=\overline{(6-x)+x}=\overline{6+((-x)+x)}=\overline{6+0}=\overline{6}=\overline{0}$$

Logo, $(\mathbb{Z}_6,+)$ é um grupo abeliano. A multiplicação em $(\mathbb{Z}_6,\cdot)$ é associativa, pois se $x,y,z\in\mathbb{Z}_6$

$$\overline{x}\cdot\left(\overline{y}\cdot\overline{z}\right)=\overline{x}\cdot\overline{y\cdot z}=\overline{x\cdot(y\cdot z)}=\overline{(x\cdot y)\cdot z}=\overline{x\cdot y}\cdot\overline{z}=\left(\overline{x}\cdot\overline{y}\right)\cdot\overline{z}$$

A distributividade da multiplicação em relação à adição é verificada em $(\mathbb{Z}_6,+,\cdot)$, pois dados $\overline{x},\overline{y},\overline{z}\in\mathbb{Z}_6$, temos que

$$\overline{x}\cdot\left(\overline{y}+\overline{z}\right)=\overline{x}\cdot\overline{y+z}=\overline{x\cdot(y+z)}=\overline{(x\cdot y)+(x\cdot z)}=\overline{x\cdot y}+\overline{x\cdot z}=\left(\overline{x}\cdot\overline{y}\right)+\left(\overline{x}\cdot\overline{z}\right)$$

$$\left(\overline{y}+\overline{z}\right)\cdot\overline{x}=\overline{y+z}\cdot\overline{x}=\overline{(y+z)\cdot x}=\overline{(y\cdot x)+(z\cdot x)}=\overline{y\cdot x}+\overline{z\cdot x}=\left(\overline{y}\cdot\overline{x}\right)+\left(\overline{z}\cdot\overline{x}\right)$$

Dessa forma, $(\mathbb{Z}_6,+,\cdot)$ corresponde a um anel. Para provar que é comutativo, observe que dados $\overline{x},\overline{y}\in\mathbb{Z}_6$, então $\overline{x}\cdot\overline{y}=\overline{x\cdot y}=\overline{y\cdot x}=\overline{y}\cdot\overline{x}$, o que prova a comutatividade da multiplicação em $(\mathbb{Z}_6,+,\cdot)$. Tomando agora $\overline{1}\in\mathbb{Z}_6$, verificamos a

validade da existência de elemento neutro em relação à multiplicação, porque para todo $\overline{x} \in \mathbb{Z}_6$, é válido que $\overline{x} \cdot \overline{1} = \overline{x \cdot 1} = \overline{x}$ e $\overline{1} \cdot \overline{x} = \overline{1 \cdot x} = \overline{x}$, de modo que $\overline{1} \in \mathbb{Z}_6$ corresponde a unidade correspondente à multiplicação em $\mathbb{Z}_6$. Portanto, $(\mathbb{Z}_6, +, \cdot)$ é um anel comutativo com unidade.

Verifiquemos agora que o anel $(\mathbb{Z}_6, +, \cdot)$ não pode ser classificado como um anel de integridade. Visto que $(\mathbb{Z}_6, +, \cdot)$ é um anel comutativo com unidade, vamos verificar que nessa estrutura não é válida a lei do anulamento do produto. Observe que $\overline{2}, \overline{3} \in \mathbb{Z}_6$ são ambos não nulos, porém, $\overline{2} \cdot \overline{3} = \overline{2 \cdot 3} = \overline{6} = \overline{0}$, ou seja, multiplicamos dois elementos não nulos de $\mathbb{Z}_6$ e obtivemos um produto nulo, isto quer dizer que $(\mathbb{Z}_6, +, \cdot)$ não goza da lei do anulamento do produto, o que não torna $(\mathbb{Z}_6, +, \cdot)$ um domínio de integridade. Temos que $\overline{2}, \overline{3} \in \mathbb{Z}_6$ podem ser classificados como divisores de zero em $(\mathbb{Z}_6, +, \cdot)$.

Por fim, a proposta é que os funcionários identifiquem algum tipo de conjunto na forma $\mathbb{Z}_m$, com m natural, que, em conjunto com as operações usuais associadas, pode ser classificado como um anel de integridade. Assim, o objetivo é avaliar se existe algum índice m natural para o qual $(\mathbb{Z}_m, +, \cdot)$ é um domínio de integridade. De modo geral, temos que $(\mathbb{Z}_m, +, \cdot)$ é um domínio de integridade se, e somente se, m for primo. Sendo $(\mathbb{Z}_m, +, \cdot)$ um domínio de integridade, se *m* não fosse primo, então teríamos $m = pq$ com *p* e *q* primos, e assim, $\mathbb{Z}_m$ conteria divisores próprios de zero, porque $\overline{p} \cdot \overline{q} = \overline{p \cdot q} = \overline{m} = \overline{0}$, o que contraria a lei da anulação do produto e, consequentemente, contraria o fato de $(\mathbb{Z}_m, +, \cdot)$ ser um domínio de integridade. Logo, m deve ser um número primo. Por outro lado, suponhamos que m é primo e sabendo que $(\mathbb{Z}_m, +, \cdot)$ é um anel comutativo com unidade para $m > 1$, ao tomarmos $\overline{a}, \overline{b} \in \mathbb{Z}_m$ tal que $\overline{a} \cdot \overline{b} = \overline{0}$ então, segue que $\overline{ab} = \overline{0}$, ou seja, ab é divisível por m, de modo que $ab = mq$ para algum $q \in \mathbb{Z}$, ou $m \mid ab$. Como m é primo, então $m \mid a$ ou $m \mid b$, o que em termos de classes de equivalência podem ser interpretados por $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$. Portanto, $(\mathbb{Z}_m, +, \cdot)$ goza da lei do anulamento do produto e, consequentemente, pode ser classificado como domínio de integridade. Por meio desse resultado, qualquer estrutura $(\mathbb{Z}_m, +, \cdot)$ com m primo será classificada como domínio de integridade, o que possibilita avaliar os exemplos que podem ser apresentados pelos funcionários durante a investigação dessa questão.

Com isso, você estará apto a finalizar as tarefas referentes ao terceiro dia, complementando o material com a indicação dos conteúdos

envolvidos e as possíveis dúvidas que podem ser apresentadas durante esse dia de curso.

Para finalizar o plano do curso de capacitação composto pelo material elaborado para os três dias de curso, faça o material que será apresentado aos funcionários na forma de slides ou material impresso e o material contendo as orientações que irão auxiliá-lo no desenvolvimento desse curso para o atendimento às dúvidas e a resolução das tarefas propostas.

Avançando na prática

Outras propriedades envolvendo os domínios de integridade

Descrição da situação-problema

Considere que você esteja trabalhando com uma turma de Ensino Médio a respeito da resolução de equações polinomiais associadas à resolução de problemas. Durante as correções de atividades relativas a esse conteúdo, você observou duas afirmações apresentadas pelos alunos, considerando que os elementos x e y, em ambos os casos, sejam números inteiros:

(a) Como $x^2 - x = 0$ então $x = 0$ ou $x = 1$.

(b) Como $xy = x$ então $y = 1$.

Analise cada afirmação apresentada, verificando, com base nas propriedades dos domínios de integridade, se a propriedade é verdadeira. E no caso de a afirmação ser falsa, apresente um contraexemplo, faça as devidas correções, justificando, e apresente um encaminhamento para auxiliar o aluno em sua dificuldade.

Resolução da situação-problema

Temos que $(\mathbb{Z}, +, \cdot)$ é um domínio de integridade, então corresponde a um anel comutativo com unidade que goza da lei do anulamento do produto. Considerando essas propriedades, analisemos as duas afirmações apresentadas:

(a) Como $x^2 - x = 0$ então $x = 0$ ou $x = 1$.

Note que $x^2 - x = 0$ pode ser reescrita como $x \cdot x - x \cdot 1 = 0$, ou ainda, $x(x-1) = 0$, pela distributividade da

multiplicação em relação à adição. Como $x, x-1 \in \mathbb{Z}$ e o produto entre eles é nulo, um desses números deve ser nulo pela lei do anulamento do produto, logo, $x=0$ ou $x-1=0$, isto é, $x=0$ ou $x=1$. Portanto, a afirmação apresentada pelo aluno está correta.

(b) Como $xy=x$, então $y=1$.

Esta afirmação é falsa, pois tomando $x=0$ e $y=3$, por exemplo, a igualdade será válida, mas $y \neq 1$. Temos que a afirmação correta é dada por: Como $xy=x$, então $y=1$ ou $x=0$. Para justificar essa afirmação, veja que $xy=x$ pode ser reescrita como $xy-x=0$, ou ainda na forma $xy-x\cdot 1=0$. Pela distributividade da multiplicação em relação à adição temos $x(y-1)=0$. Como $x, y-1 \in \mathbb{Z}$ e o produto entre eles é nulo, então um desses números deve ser nulo pela lei do anulamento do produto, logo, $x=0$ ou $y-1=0$, isto é, $x=0$ ou $y=1$.

Um encaminhamento possível seria sugerir ao aluno a verificação caso a afirmação apresentada por ele seja válida em todos os casos, solicitando que ele refletisse sobre a afirmação proposta. Quais outros encaminhamentos poderiam ser tomados nessa situação? Reflita sobre outras possibilidades de intervenção de modo a auxiliar o aluno na compreensão e na correção de seu erro.

Faça valer a pena

1. Considerando as características dos anéis e suas principais categorias, analise as seguintes afirmações, classificando-as como verdadeiras (V) ou falsas (F).

( ) Todo anel comutativo é um anel com unidade.
( ) Todo domínio de integridade é um anel.
( ) Todo anel comutativo com unidade é um domínio de integridade.
( ) Existem anéis com unidade que são anéis comutativos.
( ) Existem domínios de integridade que não são anéis comutativos.

Assinale a alternativa que indica todas as classificações corretamente, considerando a ordem na qual as afirmações foram apresentadas:

a) V – V – F – V – F.
b) V – F – F – V – V.
c) F – V – F – V – F.
d) F – V – V – F – F.
e) F – F – V – F – V.

2. As estruturas algébricas estão associadas a diversas propriedades que podem ser empregadas na resolução de problemas, na interpretação de fenômenos e na avaliação de outros objetos matemáticos derivados das estruturas em estudo.
Considere que um estudante esteja resolvendo um problema com base em uma estrutura $(A,+,\cdot)$ com *A* não vazio. Em uma das etapas da resolução do problema em questão, o estudante apresentou a seguinte afirmação: se $x \in A$ é tal que $x^2 = e_A$, então $x = e_A$.

Para que a afirmação apresentada pelo aluno seja correta, a estrutura $(A,+,\cdot)$ deve apresentar as propriedades características de qual das seguintes estruturas?

a) $(A,+,\cdot)$ deve gozar apenas das propriedades características de anel.
b) $(A,+,\cdot)$ deve gozar apenas das propriedades características de anel comutativo.
c) $(A,+,\cdot)$ deve gozar apenas das propriedades características de anel com unidade.
d) $(A,+,\cdot)$ deve gozar apenas das propriedades características de anel comutativo com unidade.
e) $(A,+,\cdot)$ deve gozar apenas das propriedades características de domínio de integridade.

3. Considere os conjuntos descritos:

$$A = \{2x+1 \mid x \in \mathbb{Z}\}$$
$$B = \{2x \mid x \in \mathbb{Z}\}$$
$$C = \left\{x + y\sqrt{3} \mid x, y \in \mathbb{Z}\right\}$$

A partir dos conjuntos apresentados, definamos as operações usuais de adição e multiplicação correspondentes, compondo, respectivamente, as estruturas $(A,+,\cdot)$, $(B,+,\cdot)$ e $(C,+,\cdot)$.

Qual(is) das estruturas apresentadas pode(m) ser classificada(s) como domínio(s) de integridade?

a) Apenas a estrutura $(C,+,\cdot)$.
b) Apenas as estruturas $(A,+,\cdot)$ e $(B,+,\cdot)$.
c) Apenas as estruturas $(A,+,\cdot)$ e $(C,+,\cdot)$.
d) Apenas as estruturas $(B,+,\cdot)$ e $(C,+,\cdot)$.
e) As estruturas $(A,+,\cdot)$, $(B,+,\cdot)$ e $(C,+,\cdot)$.

Referências

COCHMANSKI, Julio Cesar; COCHMANSKI, Liliane Cristina de Camargo. **Estruturas algébricas.** Curitiba: InterSaberes, 2016.

DOMINGUES, Hygino H.; IEZZI, Gelson. **álgebra moderna.** São Paulo: Atual, 2003.

GARCIA, Arnaldo; LEQUAIN, Yves. **Elementos de álgebra**. Rio de janeiro: IMPA, 2015.

HEFEZ, Abramo. **Curso de álgebra.** v. 1. Rio de Janeiro: IMPA, 2014.

JANESCH, Oscar Ricardo; TANEJA, Inder Jeet. **Álgebra I**. 2. ed. Florianópolis: UFSC / EAD / CED / CFM, 2011. Disponível em: <http://mtm.grad.ufsc.br/files/2014/04/%C3%81lgebra-I.pdf>. Acesso em: 10 ago. 2018.

LEITE, Álvaro Emílio; CASTANHEIRA, Nelson Pereira. **Teoria dos números e teoria dos conjuntos.** Curitiba: InterSaberes, 2014.

SANTOS, José Plínio de Oliveira. **Introdução à teoria dos números.** Rio de Janeiro: IMPA, 2015.

SELBACH, Cássio Volpato. **Uma Introdução ao estudo de anéis e corpos.** 2015. Trabalho de Conclusão de Curso (Licenciatura em Matemática) – Universidade Federal do Rio Grande do Sul, Porto Alegre.

SOUZA, Wesley Angelino de; HENRIQUE, Marco Aurélio Amaral. **Grupos, anéis e corpos e suas propriedades.** Disponível em: <http://www.dca.fee.unicamp.br/~marco/cursos/ia012_14_1/slides/grupos-aneis-corpos.pdf>. Acesso em: 10 ago. 2018.

STEWART, Ian. Em busca do infinito: **uma história da matemática dos primeiros números à teoria do caos.** Trad. George Scheslinger. 1. ed. Rio de Janeiro: Zahar, 2014.

VIEIRA, Ana Cristina. **Fundamentos de álgebra I.** Belo Horizonte: Editora UFMG, 2011

ZARPELON, Edinéia; RESENDE, Luis Mauricio Martins de; PINHEIRO, Nilcéia Aparecida Maciel. Uso de mapas conceituais na disciplina de Cálculo Diferencial e Integral 1: uma estratégia em busca da aprendizagem significativa. **Revista Brasileira de Ensino de Ciência e Tecnologia**, v. 8, n. 2, 2015. Disponível em: <https://periodicos.utfpr.edu.br/rbect/article/view/2986>. Acesso em 14 jun. 2018.

Estruturas algébricas: corpos

Convite ao estudo

Na terceira unidade deste livro foi apresentada a definição de anel em conjunto com suas propriedades características. A partir desses estudos foi possível observar que existem algumas categorias particulares que se diferenciam da definição de anel pelo acréscimo de propriedades, como é o caso dos anéis comutativos, anéis com unidade e domínios de integridade.

Nesta unidade, daremos continuidade a esse tema, observando outra subcategoria de anel essencial para o desenvolvimento de estudos em diversas áreas da Matemática: o corpo. Este conceito está presente, por exemplo, nos estudos da Álgebra Linear, do Cálculo Diferencial e Integral e da Análise Real. Assim, o conhecimento dessa estrutura algébrica é fundamental para a compreensão de outras estruturas, como o caso dos espaços vetoriais.

Nesse sentido, suponha que você atua como professor de Matemática em uma escola da educação básica. Buscando um aperfeiçoamento em seu trabalho, você começou a participar de um grupo de estudos, promovido por uma instituição de ensino superior voltado para professores de Matemática da educação básica, que visa proporcionar uma formação continuada bem como um espaço para discussões a respeito da prática docente. Os encontros são realizados mensalmente e envolvem docentes de diversas escolas e professores da instituição de ensino superior. Durante as reuniões do grupo, são propostos problemas e temas para reflexão que exigem dos professores da educação básica um aprofundamento teórico para que possam participar

das discussões propostas e observar as contribuições desses estudos para sua prática docente.

Suponha que você tenha iniciado a participação nesse grupo, em um dado semestre, a partir dos três primeiros encontros direcionados ao estudo de tópicos da Álgebra. Para o primeiro encontro, você deverá desenvolver tarefas direcionadas à comparação entre as diferentes categorias de anéis, estudando principalmente o conceito de corpo. No segundo encontro, você deverá estudar as particularidades do conjunto de polinômios e, por fim, no terceiro encontro, sua tarefa será a de analisar os homomorfismos e isomorfismos de anéis, aprofundando os estudos a respeito das funções bijetivas e sua aplicação no estudo da estrutura de anel.

Ao final dos três encontros, você deverá entregar um trabalho de conclusão de curso na forma de portfólio, no qual deverão ser inseridas todas as atividades desenvolvidas durante os três encontros em questão, além de reflexões a respeito das contribuições dos estudos realizados para o trabalho com os conteúdos matemáticos abordados na educação básica.

Para que seja possível cumprir o desafio proposto, na Seção 4.1 você estudará a estrutura de corpo, com suas propriedades características e alguns exemplos importantes. Na Seção 4.2 os estudos serão direcionados aos anéis de polinômios, enquanto na Seção 4.3 os temas a serem estudados são os homomorfismos e isomorfismos de anéis, bem como os domínios euclidianos.

Dando continuidade à leitura, verifique os conhecimentos essenciais que você e os demais integrantes do grupo precisam estudar para desenvolver as propostas de estudo apresentadas nesses três primeiros encontros.

Seção 4.1

Estruturas algébricas: estudo dos corpos

Diálogo aberto

Nesta seção discutiremos a respeito das principais categorias de anéis, destacando o conceito de corpo, o qual está presente no estudo da Álgebra Linear, do Cálculo Diferencial e Integral, entre outros, fato este que se torna evidente quando abordamos conteúdos que envolvem vetores e espaços vetoriais, os quais são estudados em associação com um corpo e outros elementos.

Para isso, considere o contexto de participação em um grupo de estudos para professores de Matemática, promovido por uma instituição de ensino superior. No primeiro encontro do semestre foi proposto um estudo sobre tópicos da Álgebra, iniciando pela análise dos anéis e corpos, o qual será complementado nos próximos dois encontros.

Para desenvolver a proposta do primeiro encontro, a turma foi dividida em grupos e você ficou responsável, em conjunto com seus colegas, por analisar as diferentes categorias de anéis e as inclusões existentes entre elas. Assim, sua tarefa consiste em identificar exemplos de conjuntos, com operações, que possibilitam a identificação de relações de inclusão entre as seguintes categorias: anel, anel comutativo com unidade, domínio de integridade e corpo, destacando exemplos de anéis que pertençam a uma categoria, mas que não possam ser incluídos nas categorias mais específicas, ou seja, nas categorias que apresentam um conjunto maior de propriedades.

Após essa construção, considerando o conceito de corpo, você e seu grupo precisarão resolver o seguinte problema: prove que o conjunto $\mathbb{Q}\sqrt{2} = \left\{a + b\sqrt{2};\ a,b \in \mathbb{Q}\right\}$, com as operações usuais de adição e multiplicação derivada do conjunto dos números reais, é um corpo. O estudo desse tipo de estrutura pode favorecer a compreensão da propriedade da existência de elemento simétrico relativo à multiplicação, principalmente quando são estudados os números reais que não são racionais, como o caso de $\sqrt{2}$ e $\sqrt{3}$, por

exemplo, o que também pode contribuir para a compreensão do processo empregado para a identificação dos inversos multiplicativos para os números complexos não nulos.

Para finalizar as tarefas desse primeiro encontro, organize um texto contendo todas as informações empregadas para o desenvolvimento das tarefas propostas. Utilize esquemas que favoreçam a visualização e a compreensão das relações estabelecidas entre as categorias de anéis. Elabore também um material para que seja possível realizar uma breve apresentação para os colegas de grupo a respeito dos temas estudados por vocês.

Não pode faltar

Na unidade anterior estudamos a definição de anel e a caracterização de algumas subcategorias (anel comutativo, anel com unidade e domínio de integridade). Observamos que a construção dessas subcategorias se dá a partir do acréscimo de propriedades relativas à segunda operação binária definida sobre o conjunto em estudo. Assim, todas as subcategorias admitem as mesmas propriedades com relação à primeira operação, mas diferenciam-se quando avaliamos as propriedades verificadas pela segunda operação binária.

Quando estudamos o anel dos inteiros, $(\mathbb{Z},+,\cdot)$, verificamos que ele pode ser classificado como domínio de integridade. Dessa forma, $(\mathbb{Z},+,\cdot)$, em particular, é um anel comutativo com unidade, o que implica $(\mathbb{Z},\cdot)$ gozar do fechamento, associatividade, comutatividade e existência de elemento neutro. Quando comparamos essa estrutura com $(\mathbb{Z},\cdot)$, verificamos que a única propriedade ainda não estudada é a existência de elemento simétrico em relação à multiplicação para todo inteiro. Mas será que essa propriedade é válida nessa estrutura? Como a presença, ou não, dessa propriedade influencia no estudo de $(\mathbb{Z},+)$ enquanto estrutura algébrica?

Para responder a esses questionamentos, vamos estudar outra estrutura algébrica importante derivada dos anéis, a qual é denominada de corpo. Essa é uma das estruturas utilizada, por exemplo, quando desejamos aumentar ou reduzir o comprimento de um vetor no plano ou no espaço, por possibilitar a definição da operação de multiplicação por escalar quando estudamos um

espaço vetorial. O termo escalar, nesse contexto, diz respeito a um elemento de um corpo, tomado de acordo com a finalidade dos estudos a serem desenvolvidos.

Considerando a aplicabilidade desse conceito em estudos da Matemática e também de outros campos do conhecimento, vamos agora estudar que propriedades caracterizam um corpo, tomando como base os estudos sobre anéis que foram realizados anteriormente.

Conceito de corpo

Considere um anel $(K,+,\cdot)$ comutativo com unidade. Se todo elemento não nulo de K admitir um elemento simétrico em relação à operação $\cdot$, então podemos dizer que $(K,+,\cdot)$ é um **corpo**.

Dado $a \in K$, se existe $b \in K$, tal que $a \cdot b = 1_K$, em que 1_K corresponde à unidade do anel com unidade $(K,+,\cdot)$, então dizemos que *a* é um **elemento inversível** de *K* e que *b* é o **elemento inverso** de *a*. Nesse caso, podemos denotar $b = a^{-1}$. Assim, podemos reescrever a definição de corpo da seguinte forma: o anel comutativo com unidade $(K,+,\cdot)$ será chamado de corpo se todo elemento não nulo de *K* for inversível.

Assimile

Ao comparar a definição de corpo com a estrutura de grupo, podemos observar que $(K,+,\cdot)$ será um corpo quando satisfizer as seguintes condições: $(K,+)$ for um grupo abeliano; $(K^*,\cdot)$ for um grupo abeliano, onde $K^* = K - \{e_k\}$, com e_k sendo o elemento neutro da operação $+$; e $(K,+,\cdot)$ gozar da distributividade da operação $\cdot$ em relação à $+$.

Como estudado anteriormente, $(\mathbb{Z},+,\cdot)$ corresponde a um anel comutativo com unidade. Porém, nessa estrutura, apenas os números -1 e 1 são inversíveis, pois $(-1)(-1) = 1$ e $1 \cdot 1 = 1$, fazendo com que -1 seja inverso -1 e 1 seja inverso 1, considerando a multiplicação de inteiros. Para todos os demais números inteiros *a* não nulos, não é possível identificar outro inteiro *b* de modo que $a \cdot b = 1$. Como existem números inteiros não nulos que não admitem

inverso, podemos concluir que $(\mathbb{Z}^*,\cdot)$ não goza da existência de um elemento simétrico a todo número inteiro não nulo, portanto, $(\mathbb{Z},+,\cdot)$ não pode ser classificado como corpo.

Os principais exemplos de corpos que podemos destacar são aqueles derivados dos conjuntos numéricos, como é o caso de $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ e $(\mathbb{C},+,\cdot)$. Por exemplo, note que $(\mathbb{Q},+,\cdot)$ é um anel comutativo com unidade, conforme discutido anteriormente. Além disso, dado qualquer número racional não nulo *a*, podemos identificar seu inverso $a^{-1}=\frac{1}{a}$ com $a\cdot\frac{1}{a}=\frac{1}{a}\cdot a=1$, ou seja, todo racional não nulo admite inverso multiplicativo, comprovando que $(\mathbb{Q}^*,\cdot)$ é um grupo abeliano porque goza do fechamento, associatividade, comutatividade, existência de elemento neutro e existência de elemento simétrico a todo racional não nulo. Assim, $(\mathbb{Q},+,\cdot)$ corresponde a um corpo. Argumentos análogos podem ser empregados no estudo de $(\mathbb{R},+,\cdot)$ e $(\mathbb{C},+,\cdot)$.

Exemplificando

Considere o anel $(\mathbb{R}^{\mathbb{R}},+,\cdot)$ das funções reais de uma variável com suas operações usuais. Essa estrutura, como estudado na unidade anterior, pode ser classificada como anel comutativo com unidade, sendo sua unidade a função $u:\mathbb{R}\to\mathbb{R}$ definida por $u(x)=1$ para todo *x* real.

De posse dessa estrutura, seja a função $f:\mathbb{R}\to\mathbb{R}$ definida por

$$f(x)=\begin{cases}0, \text{ se } x=0\\ 2, \text{ se } x\neq 0\end{cases}$$

Como *f* é não nula, então *f* não corresponde ao elemento neutro da adição em $\mathbb{R}^{\mathbb{R}}$. Dessa forma, dada qualquer $g:\mathbb{R}\to\mathbb{R}$, temos que

$$(fg)(0)=f(0)g(0)=0\cdot g(0)=0$$

Isto é, $fg\neq u$. Logo, *f* não é inversível.

Sendo assim, como existe *f* não nula em $\mathbb{R}^{\mathbb{R}}$, que não admite inversa em relação à multiplicação, podemos concluir que $(\mathbb{R}^{\mathbb{R}},+,\cdot)$ não é um corpo.

Na definição de corpo, observamos a indicação de propriedades que devem ser verificadas pela estrutura em questão de modo a

possibilitar sua caraterização. No entanto, outras relações podem ser estabelecidas como consequências dessa definição.

Propriedades dos corpos

Além das propriedades que definem os corpos, existem outras que podem ser estabelecidas como consequências da definição e que possibilitam relacionar os corpos com outras categorias de anéis, conforme indicado nas seguintes proposições.

Proposição 1: Todo corpo é um domínio de integridade.

Demonstração: Se $(K,+,\cdot)$ é um corpo, então, pode ser classificado como um anel comutativo com unidade. Assim, para provar que $(K,+,\cdot)$ é um domínio de integridade, basta verificar se é válida a lei do anulamento do produto. Para isso, sejam $a,b \in K$, tais que $a \cdot b = e_k$, com e_k sendo o elemento neutro da operação $+$ definida sobre *K*. Se $a = e_k$, não há o que provar. Supondo $a \neq e_k$, então *a* é inversível e admite um elemento inverso a^{-1}. Multiplicando ambos os membros de $a \cdot b = e_k$ por a^{-1}, segue que

$$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot e_k = e_k \quad \Rightarrow \quad (a^{-1} \cdot a) \cdot b = e_k \quad \Rightarrow \quad 1 \cdot b = e_k \quad \Rightarrow \quad b = e_k$$

Isto é, $b = e_k$. De modo análogo, supondo $b \neq e_k$, então *b* será inversível e, assim, $a = e_k$. Portanto, se $a \cdot b = e_k$, um dos fatores (*a* ou *b*) deve ser nulo, ou seja, igual ao elemento neutro e_k da operação $+$ de *K*, o que comprova o fato de $(K,+,\cdot)$ gozar da lei do anulamento do produto, ou seja, de $(K,+,\cdot)$ ser um domínio de integridade.

Reflita

Na proposição 1 verificamos que todo corpo é um domínio de integridade. Mas será que a recíproca dessa afirmação é válida? Podemos afirmar que todo domínio de integridade é um corpo?

A relação entre os domínios de integridade e corpos também pode ser estudada com base em algumas características do conjunto que compõe essas estruturas, principalmente quando consideramos conjuntos finitos, ou seja, aqueles que possuem uma quantidade finita de elementos. Dessa forma, verifiquemos a seguir outra associação possível entre os domínios de integridade e os corpos.

Proposição 2: Todo domínio de integridade finito é um corpo.

Demonstração: Seja um domínio de integridade $(A,+,\cdot)$, no qual $A=\{e_k, a_1, a_2, \ldots, a_n\}$, isto é, *A* é finito. Considere $a \in A-\{e_k\}$, com e_k sendo o elemento neutro da operação $+$, o qual existe porque estamos considerando um domínio de integridade. Veja que *a* é um elemento não nulo em *A*, por ser diferente de e_k. A unidade $1_A \in A$, porque $(A,+,\cdot)$ é um domínio de integridade e, em particular, um anel com unidade. A partir de *a*, vamos construir os produtos $aa_1, aa_2, \ldots, aa_n$, os quais são distintos dois a dois, pois, se $aa_j = aa_k$, ou ainda, $a(a_j - a_k) = e_k$, por ser domínio de integridade e *a* ser não nulo, então $a_j = a_k$. Os produtos construídos com base em *a* percorrem todos os elementos não nulos de *A*, de tal forma que existe algum *i* tal que $aa_i = 1_A$, o que significa que *a* é inversível, e sendo *a* um elemento não nulo qualquer de *A*, podemos concluir que todo elemento não nulo de *A* é inversível, assim, $(A,+,\cdot)$ pode ser classificado como corpo, comcluindo essa demonstração.

Exemplificando

Seja o anel $(\mathbb{Z}_m,+,\cdot)$ das classes de restos da divisão por *m*, com *m* sendo um número natural.

Vamos considerar $m=3$, de modo a construir as tábuas das operações correspondentes ao anel $(\mathbb{Z}_3,+,\cdot)$, conforme apresentado na Figura 4.1.

Figura 4.1 | Tábuas associadas ao anel $(\mathbb{Z}_3,+,\cdot)$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

Fonte: elaborada pela autora.

Note que a multiplicação definida sobre $(\mathbb{Z}_3,+,\cdot)$, conforme a tábua presente na Figura 4.1, não apresenta divisores de zero, ou seja, não

é possível identificar dois elementos $\bar{x}$ e $\bar{y}$ de $\mathbb{Z}_3$, ambos não nulos, de tal forma que $\bar{x}\cdot\bar{y}=\bar{0}$. Por outro lado, seja $m=4$ e as tábuas associadas às operações definidas sobre o anel $(\mathbb{Z}_4,+,\cdot)$, conforme apresentado na Figura 4.2.

Figura 4.2 | Tábuas associadas ao anel $(\mathbb{Z}_4,+,\cdot)$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Fonte: elaborada pela autora.

No caso de $(\mathbb{Z}_4,+,\cdot)$, se tomarmos $\bar{2}\in\mathbb{Z}_4$, teremos $\bar{2}\cdot\bar{2}=\bar{0}$, ou seja, um produto que envolve fatores não nulos e que resulta em $\bar{0}$, sendo que, nesse caso, $\bar{2}$ é chamado de divisor de zero em $\mathbb{Z}_4$.

Essa diferença entre os anéis $(\mathbb{Z}_3,+,\cdot)$ e $(\mathbb{Z}_4,+,\cdot)$ se deve ao fato de que tomando $(\mathbb{Z}_m,+,\cdot)$, com *m* um número composto (não primo), mostra que $(\mathbb{Z}_m,+,\cdot)$ admite divisores de zero, ou seja, não pode ser classificado como domínio de integridade. Por outro lado, se temos $(\mathbb{Z}_p,+,\cdot)$, com *p* sendo um número primo, então, $(\mathbb{Z}_p,+,\cdot)$ pode ser classificado como domínio de integridade.

Considerando agora a estrutura $(\mathbb{Z}_p,+,\cdot)$ com *p* número primo, a qual é um domínio de integridade, note que o conjunto $\mathbb{Z}_p$ é finito, podendo ser descrito por $\mathbb{Z}_p=\{\bar{0},\ \bar{1},\ \bar{2},\ \ldots,\ \overline{p-1}\}$. Portanto, como $(\mathbb{Z}_p,+,\cdot)$ é um domínio de integridade finito, podemos concluir, pela proposição 2, que $(\mathbb{Z}_p,+,\cdot)$ é um corpo.

As proposições 1 e 2 possibilitam a comparação entre as estruturas dos domínios de integridade e corpos, relacionando as propriedades entre si com base, principalmente, nas características do conjunto em estudo.

Outra propriedade que também pode ser verificada no estudo dos corpos diz respeito à resolução de equações com base em suas propriedades, como indicado no seguinte resultado.

Propriedade 1: Em um corpo $(K,+,\cdot)$, equação $a\cdot x=b$, com $a\neq e_k$, tem solução única. A solução apresenta a forma $x=a^{-1}\cdot b$.

Demonstração: Considere que a equação $a\cdot x=b$, com $a\neq e_k$, admita soluções $x,y\in K$. Nesse caso, temos que $a\cdot x=b$ e $a\cdot y=b$. Como $(K,+,\cdot)$ é corpo, $a\neq e_k$ admite elemento inverso a^{-1} de tal forma que

$$x=\left(a^{-1}\cdot a\right)\cdot x=a^{-1}\cdot(a\cdot x)=a^{-1}\cdot b=a^{-1}\cdot(a\cdot y)=\left(a^{-1}\cdot a\right)\cdot y=y$$

Sendo assim, $x=y$ e a equação $a\cdot x=b$ apresenta solução única, a qual é dada por $x=a^{-1}\cdot b$ pela existência do simétrico a^{-1} do elemento não nulo *a* de *K*.

Essas são propriedades que possibilitam o estudo da estrutura de corpo, relacionada a diferentes conjuntos com operações, e que favorecem a sua comparação com outras estruturas, verificando a aplicabilidade de cada uma delas de acordo com o tipo de problema a ser resolvido.

Reflita

Note que cada subcategoria de anel apresenta propriedades particulares, mas que todas possuem algumas propriedades em comum, que são aquelas correspondentes à definição de anel. Analisando as diferentes subcategorias estudadas, que semelhanças e diferenças podemos identificar? Quais os principais exemplos associados a cada subcategoria? De que forma essas subcategorias influenciam, por exemplo, na resolução de equações polinomiais?

A partir da definição e dos resultados apresentados, podemos estudar outras estruturas de modo a investigar a validade ou não das propriedades características de um corpo.

Considere, por exemplo, o anel das matrizes quadradas com entradas reais $(M_n(\mathbb{R}),+,\cdot)$, que já foi estudado anteriormente. Essa estrutura goza das propriedades características de um anel e admite unidade para a multiplicação de matrizes, que corresponde à matriz

identidade de ordem n, o que implica em $(M_n(\mathbb{R}),+,\cdot)$ ser caracterizado como anel com unidade. No entanto, como a multiplicação de matrizes não é comutativa, $(M_n(\mathbb{R}),+,\cdot)$, não pode ser classificado como anel comutativo. Devido à ausência da comutatividade da multiplicação de matrizes, podemos concluir que $(M_n(\mathbb{R}),+,\cdot)$ não é um corpo, porque, em particular, $(M_n(\mathbb{R}),+,\cdot)$ precisaria ser um anel comutativo com unidade, o que não ocorre nesse caso.

Note que todas as propriedades da definição de corpo devem ser verificadas para que uma estrutura seja classificada como corpo. Assim, não basta que a estrutura goze da existência de elemento simétrico para todo elemento não nulo em relação à segunda operação binária, é essencial que a estrutura seja, a princípio, um anel comutativo com unidade.

Outro estudo que podemos realizar considerando a estrutura de corpo consiste em avaliar subconjuntos de modo análogo às relações entre anéis e subanéis. Assim, temos o conceito de subanel.

Subcorpos

Considere $(K,+,\cdot)$ um corpo e $L \subset K$ um subconjunto não vazio. A estrutura $(L,+,\cdot)$ será chamada de **subcorpo** de $(K,+,\cdot)$ quando $(L,+,\cdot)$ gozar do fechamento das duas operações binárias e, além disso, $(L,+,\cdot)$ apresentar uma estrutura de corpo quando tomamos as operações de K restritas ao conjunto L.

Como exemplo, podemos destacar $(\mathbb{Q},+,\cdot)$ e $(\mathbb{R},+,\cdot)$, já que $(\mathbb{Q},+,\cdot)$ pode ser interpretado como um subcorpo de $(\mathbb{R},+,\cdot)$.

Devido às relações existentes entre um corpo e seus subcorpos, podemos empregar a seguinte proposição como uma forma equivalente para identificar subcorpos a partir de uma estrutura de corpo.

Proposição 3: Sejam $(K,+,\cdot)$ um corpo e $L \subset K$ um subconjunto não vazio. Para que $(L,+,\cdot)$ seja um subcorpo de $(K,+,\cdot)$, é necessário e suficiente que as seguintes condições sejam válidas:

- $e_K, 1_K \in L$, com e_K e 1_K sendo, respectivamente, os elementos neutros das operações $+$ e $\cdot$ de K restritas a L, quando não existir possibilidade de confusão quanto à notação, podemos adotar e ou 0 como elemento neutro referente à operação $+$ e 1 como a unidade correspondente ao elemento neutro associado à operação $\cdot$.

- Se $x, y \in L$, então $x - y \in L$.
- Se $x, y \in L$ e $y \neq e_K$, então $x \cdot y^{-1} \in L$.

Como sugestão de estudo complementar, construa uma demonstração para a proposição 3 com base nos conhecimentos a respeito das estruturas algébricas, e relacionando com os resultados relativos aos subgrupos e subanéis.

Assimile

Para comprovar que um subconjunto não vazio associado a um corpo compõe um subcorpo, considerando as restrições das operações que definem o corpo, podemos empregar as condições presentes na definição ou comprovar as condições indicadas na proposição 3, ou seja, o subcorpo deve conter os elementos neutros referentes às duas operações, ser fechado considerando a diferença de elementos e ser fechado para a multiplicação de um elemento pelo inverso de um outro elemento não nulo.

Um exemplo importante de subcorpo é a estrutura $(\mathbb{Q}, +, \cdot)$, que pode ser classificada como subcorpo de $(\mathbb{R}, +, \cdot)$, que por sua vez pode ser interpretado como subcorpo de $(\mathbb{C}, +, \cdot)$.

Faça você mesmo

Dentre as estruturas estudadas anteriormente, identifique outros exemplos de corpos e subcorpos associados. Identifique também exemplos de subconjuntos, associados a corpos e que não compõem estruturas que podem ser classificadas como subcorpos.

Pesquise mais

Para complementar os estudos a respeito dos anéis e corpos, consulte a seção 1.2, localizada entre as páginas 18 e 25 do material intitulado Álgebra I, de Oscar Ricardo Janesch e Inder Jeet Taneja. Disponível em: <http://mtm.grad.ufsc.br/files/2014/04/%C3%81lgebra-I.pdf>. Acesso em: 12 set. 2018.

Os capítulos 1, 2 e 3 deste mesmo material podem contribuir com os estudos realizados a respeito dos anéis e suas subcategorias.

Sem medo de errar

Para o primeiro encontro do grupo de estudos, você e seus colegas deverão executar uma tarefa dividida em duas partes: a primeira consiste em comparar as diferentes subcategorias de anéis entre si, identificando exemplos correspondentes, já a segunda refere-se a provar que $\left(\mathbb{Q}\sqrt{2},+,\cdot\right)$ é um corpo.

Sendo assim, para a primeira parte, você e seu grupo devem identificar exemplos de conjuntos, com operações, que possibilitam uma comparação entre anéis, anéis comutativos com unidade, domínios de integridade e corpos. Nesse caso, podem ser construídos diagramas, com base na Teoria de Conjuntos, a fim de evidenciar as relações de inclusão entre essas categorias.

Vamos iniciar esse estudo pelo conjunto de anéis. Dentre todas as categorias citadas anteriormente, a estrutura de anel é aquela que fundamenta todas as demais e que envolve a maior parte dos exemplos, por se tratar de uma categoria com um menor conjunto de propriedades a serem satisfeitas quando comparado com as categorias particulares.

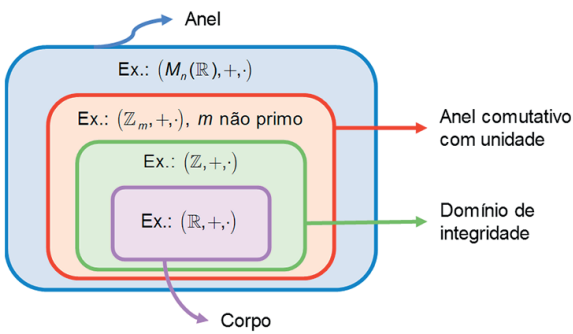
Os anéis comutativos com unidade correspondem aos anéis que gozam também das propriedades comutativa e existência de elemento neutro quando avaliamos a segunda operação binária que compõe a estrutura. Nesse sentido, temos que todo anel comutativo com unidade é um anel, porém, nem todo anel pode ser classificado como comutativo com unidade, como é o caso do anel composto pelas matrizes quadradas de ordem *n* com entradas reais munido das operações usuais de adição e multiplicação de matrizes e denotado por $\left(M_n(\mathbb{R}),+,\cdot\right)$. Sabemos que a multiplicação de matrizes não é comutativa, então $\left(M_n(\mathbb{R}),+,\cdot\right)$ não pertence ao conjunto dos anéis comutativos com unidade. Dessa análise, podemos concluir que o conjunto dos anéis comutativos com unidade está contido no conjunto dos anéis.

Os domínios de integridade são anéis comutativos com unidade que não possuem divisores de zero, ou que gozam da lei do anulamento do produto. Note que nem todo anel comutativo com unidade é um domínio de integridade, como é o caso do anel das classes de restos $\left(\mathbb{Z}_m,+,\cdot\right)$ quando *m* não é primo, dentre os quais podemos destacar o $\left(\mathbb{Z}_4,+,\cdot\right)$. Esse tipo de estrutura é um anel comutativo com unidade que possui divisores de zero, então, não pode ser classificado como domínio de integridade. A partir dessa informação, podemos concluir

que o conjunto dos domínios de integridade está contido no conjunto dos anéis comutativos com unidade.

Os corpos são anéis comutativos com unidade em que todo elemento não nulo admite inverso em relação à segunda operação binária, como é o caso de $(\mathbb{R},+,\cdot)$, por exemplo. Conforme a proposição 1, ainda temos que todo corpo é um domínio de integridade. Porém, nem todo domínio de integridade é um corpo, que é o caso de $(\mathbb{Z},+,\cdot)$, um domínio de integridade mas que possui apenas os elementos -1 e 1 inversíveis. Logo, o conjunto dos corpos está contido no conjunto dos domínios de integridade. Podemos ilustrar essas relações de inclusão por meio de um diagrama, conforme o apresentado na Figura 4.3.

Figura 4.3 | Relações de inclusão entre as subcategorias de anéis



Fonte: elaborada pela autora.

A segunda parte da tarefa direcionada ao seu grupo consiste em provar que o conjunto $\mathbb{Q}\sqrt{2}=\left\{a+b\sqrt{2};\ a,b\in\mathbb{Q}\right\}$, com as operações usuais de adição e multiplicação derivada do conjunto dos números reais, é um corpo, ou seja, que $\left(\mathbb{Q}\sqrt{2},+,\cdot\right)$ é um corpo. Podemos empregar duas estratégias nesse caso. A primeira é mostrando que $\left(\mathbb{Q}\sqrt{2},+,\cdot\right)$ é um corpo a partir da definição e, nesse caso, verificamos cada uma das propriedades de forma independente, provando que $\left(\mathbb{Q}\sqrt{2},+,\cdot\right)$ é um anel comutativo com unidade e que a multiplicação goza da existência de elemento simétrico a todo elemento não nulo de $\mathbb{Q}\sqrt{2}$. A segunda consiste em provar que $\left(\mathbb{Q}\sqrt{2},+,\cdot\right)$ é um subcorpo de $(\mathbb{R},+,\cdot)$, porque $\mathbb{Q}\sqrt{2}\subset\mathbb{R}$ e também se $\left(\mathbb{Q}\sqrt{2},+,\cdot\right)$ for

subcorpo então, em particular, será um corpo. Vamos empregar esse segundo procedimento para estudar o anel $\left(\mathbb{Q}\sqrt{2},+,\cdot\right)$ com base nas condições indicadas na proposição 3.

Note que o elemento neutro da adição ($0\in\mathbb{R}$) e o elemento neutro da multiplicação ($1\in\mathbb{R}$), nos reais, são elementos de $\mathbb{Q}\sqrt{2}$, porque $0=0+0\sqrt{2}\in\mathbb{Q}\sqrt{2}$ e $1=1+0\sqrt{2}\in\mathbb{Q}\sqrt{2}$. Considere agora $x=a+b\sqrt{2}\in\mathbb{Q}\sqrt{2}$ e $y=c+d\sqrt{2}\in\mathbb{Q}\sqrt{2}$, e assim, considerando a restrição da adição sobre $\mathbb{Q}\sqrt{2}$, teremos $x-y=\left(a+b\sqrt{2}\right)-\left(c+d\sqrt{2}\right)=(a-c)+(b-d)\sqrt{2}$, com $a-c,b-d\in\mathbb{Q}$. Dessa forma, $x,y\in\mathbb{Q}\sqrt{2}$. Além disso, se $x,y\in\mathbb{Q}\sqrt{2}$ com $y\neq 0$, esses elementos podem ser representados como $x=a+b\sqrt{2}\in\mathbb{Q}\sqrt{2}$ e $y=c+d\sqrt{2}\in\mathbb{Q}\sqrt{2}$, de modo que $c\neq 0$ ou $d\neq 0$. Sendo assim,

$$xy^{-1}=\left(a+b\sqrt{2}\right)\cdot\frac{1}{c+d\sqrt{2}}=\frac{a+b\sqrt{2}}{c+d\sqrt{2}}=\left(\frac{a+b\sqrt{2}}{c+d\sqrt{2}}\right)\cdot\left(\frac{c-d\sqrt{2}}{c-d\sqrt{2}}\right)$$

$$=\frac{(ac-2bd)+(bc-ad)\sqrt{2}}{c^2-2d^2}=\frac{ac-2bd}{c^2-2d^2}+\frac{bc-ad}{c^2-2d^2}\sqrt{2}$$

Veja que $c^2-2d^2\neq 0$, pois, caso contrário, $c/d=\sqrt{2}$, o que é impossível, visto que $c,d\in\mathbb{Q}$. Como $\frac{ac-2bd}{c^2-2d^2}$ e $\frac{bc-ad}{c^2-2d^2}$ são números racionais, então $xy^{-1}\in\mathbb{Q}\sqrt{2}$. Portanto, pela proposição 3, $\left(\mathbb{Q}\sqrt{2},+,\cdot\right)$ é um subcorpo de $(\mathbb{R},+,\cdot)$ e, em particular, $\left(\mathbb{Q}\sqrt{2},+,\cdot\right)$ é um corpo.

Para finalizar sua tarefa, elabore um documento com um resumo a respeito dos tópicos estudados por seu grupo e construa uma breve apresentação para que você e seu grupo possam iniciar as discussões com os demais docentes a respeito dos temas estudados por vocês.

Avançando na prática

O estudo do plano complexo e a estrutura de corpo

Descrição da situação-problema

O conjunto dos números complexos pode ser interpretado como o conjunto dos pares ordenados **(a, b)** de números reais, cuja representação geométrica pode ser dada a partir do plano complexo, o qual possui estrutura semelhante à do plano cartesiano,

sendo este a representação geométrica de $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$. Imagine que você pretende trabalhar com as representações geométricas e com as operações usuais definidas sobre o conjunto dos números complexos com uma turma de Ensino Médio. Ao selecionar as tarefas a serem desenvolvidas em sala, você deparou-se com a seguinte proposta: é possível identificar um número complexo (x, y) não nulo de modo que $(0,1) \cdot (x, y) = (0,0)$? Considerando a tarefa descrita, como você responderia ao questionamento proposto, considerando as propriedades apresentadas pela estrutura $(\mathbb{C}, +, \cdot)$? Quais dúvidas poderiam surgir durante a aplicação dessa tarefa à turma do Ensino Médio e quais encaminhamentos poderiam ser adotados?

Resolução da situação-problema

O conjunto dos números complexos, com suas operações usuais de adição e multiplicação, pode ser classificado como um corpo. Considerando a representação enquanto par ordenado, as operações de adição e multiplicação usuais podem ser representadas, respectivamente, como $(a, b) + (c, d) = (a + c, b + d)$ e $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$, para todos $(a, b), (c, d) \in \mathbb{C}$.

Por se tratar de um corpo, $(\mathbb{C}, +, \cdot)$ pode ser classificado, em particular, como um domínio de integridade, logo, em $(\mathbb{C}, +, \cdot)$ não é possível identificar divisores de zero. Com essa informação, temos que não é possível identificar (x, y) não nulo de modo que $(0,1) \cdot (x, y) = (0,0)$, pois $(0,1)$ é também não nulo.

No entanto, os alunos podem encontrar conclusões distintas caso não empreguem a definição correta da operação de multiplicação de números complexos que o define como corpo.

Por exemplo, alguns alunos podem interpretar o resultado do produto $(0,1) \cdot (x, y)$ como o número complexo $(0 \cdot x, 1 \cdot y)$, empregando a multiplicação entre coordenadas correspondentes. Se adotarem esse tipo de multiplicação, ao igualar $(0 \cdot x, 1 \cdot y)$ a $(0,0)$ seria possível identificar, por exemplo, o número complexo $(2,0)$, tal que $(0,1) \cdot (2,0) = (0 \cdot 2, 1 \cdot 0) = (0,0)$ e, nesse caso, $(x, y) = (2,0)$. No entanto, com essa multiplicação não teríamos a caracterização de $\mathbb{C}$, em conjunto com a adição, enquanto corpo. Para esse tipo de situação, é importante a intervenção do professor de modo a

evidenciar qual a operação de multiplicação adequada com o conjunto em questão e a representação enquanto par ordenado.

Para a conclusão dessa tarefa, organize a resolução da tarefa apresentada, acrescentando comentários a respeito do conteúdo abordado e indicando outras dificuldades que podem surgir durante a aplicação da tarefa e os encaminhamentos a serem adotados pelo professor.

Faça valer a pena

1. Com base nas principais características dos anéis, anéis comutativos com unidade, domínios de integridade e corpos, complete as lacunas das seguintes afirmações de modo a torná-las informações corretas a respeito do assunto:

I. Todo _____ pode ser classificado como um corpo.
II. Em um corpo todo _____ do conjunto deve ser inversível.
III. A unidade de um corpo é _____ zero do corpo.

Assinale a alternativa que indica os termos que completam corretamente as lacunas das afirmações apresentadas.

a) I – anel de integridade; II – elemento não nulo; III – diferente do.
b) I – anel com unidade; II – elemento não nulo; III – igual ao.
c) I – anel comutativo; II – elemento; III – diferente do.
d) I – anel de integridade finito; II – elemento; III – igual ao.
e) I – anel de integridade finito; II – elemento não nulo; III – diferente do.

2. Considere um conjunto $A = \{a, b\}$ composto por dois elementos, sobre o qual são definidas duas operações binárias, $+$ e $\cdot$, cujas tábuas de operação são indicadas na Figura 4.4.

Figura 4.4 | Tábuas de operações de $(A, +, \cdot)$

$+$	a	b
a	a	b
b	b	a

$\cdot$	a	b
a	a	a
b	a	b

Fonte: elaborada pela autora.

Em relação à estrutura apresentada e suas tábuas correspondentes, analise as seguintes afirmações:

I. A estrutura $(A,+,\cdot)$ pode ser classificada como um anel comutativo.
II. A unidade da estrutura $(A,+,\cdot)$ corresponde ao elemento a.
III. A estrutura $(A,+,\cdot)$ pode ser classificada como um corpo.

A respeito das afirmações apresentadas, assinale a alternativa correta.
a) Apenas a afirmação II está correta.
b) Apenas a afirmação III está correta.
c) Apenas as afirmações I e II estão corretas.
d) Apenas as afirmações I e III estão corretas.
e) Apenas as afirmações II e III estão corretas.

3. Considere o conjunto dos números racionais $\mathbb{Q}$ munido das seguintes operações:

$$x \oplus y = x + y - 1$$
$$x \otimes y = x + y - xy$$

para todos $x, y \in \mathbb{Q}$. Note que as operações $\oplus$ e $\otimes$ são definidas a partir das operações usuais definidas sobre $\mathbb{Q}$.
Com base nas características da estrutura $(\mathbb{Q},\oplus,\otimes)$, analise as seguintes afirmações classificando-as como verdadeiras (V) ou falsas (F):
( ) A estrutura $(\mathbb{Q},\oplus,\otimes)$ goza da comutatividade da operação $\otimes$.
( ) Todo número racional não nulo é inversível, ou seja, admite inverso em relação à operação $\otimes$.
( ) A estrutura $(\mathbb{Q},\oplus,\otimes)$ pode ser classificada como um corpo.

A partir das afirmações apresentadas, assinale a alternativa que indica todas as classificações corretamente, considerando a ordem na qual as afirmações foram apresentadas:

a) V – F – F.
b) V – V – F.
c) V – F – V.
d) F – V – F.
e) F – F – V.

Seção 4.2

Anéis de polinômios

Diálogo aberto

Na seção anterior estudamos a definição de corpo e observamos as relações existentes entre as subcategorias de anéis. Com base na estrutura de anel e de corpo, nesta seção estudaremos os polinômios, que fazem parte de um conteúdo matemático abordado desde os anos finais do ensino fundamental, sendo essencial também para os currículos de Matemática do ensino médio. Os polinômios são empregados no cálculo de áreas e volumes, no ajuste de curvas, entre outros, o que possibilita sua aplicação nas mais variadas áreas, como na Física e nas Engenharias.

Considerando o contexto envolvendo a participação em um grupo de estudos proposto por uma instituição de Ensino Superior como formação continuada para professores da Educação Básica, o segundo encontro apresentou como tema central o estudo dos polinômios, um dos conceitos essenciais para a Álgebra, inclusive na educação básica, etapa na qual são abordados os conceitos iniciais em associação com aplicações práticas, como é o caso do lançamento de projéteis, a descrição de retas no plano, entre outros.

No segundo encontro, você e outros dois colegas ficaram responsáveis por estudar dois temas relacionados aos polinômios e apresentá-los aos demais integrantes. A primeira tarefa que vocês devem desenvolver consiste em analisar a estrutura dos polinômios e identificar quais são as vantagens em construí-los com base em conjuntos com operações que são classificados como corpos em vez de tomar apenas os anéis em geral. Nesse caso, vocês devem relacionar os polinômios com o tema abordado no primeiro encontro do grupo.

A segunda tarefa, por sua vez, consiste em estudar as equações polinomiais de 2º grau e seu método de resolução característico. Considerando os conteúdos abordados na educação básica, um tema essencial para o estudo são os métodos de resolução das equações polinomiais. A fórmula de resolução da equação do 2º

grau é abordada desde o ensino fundamental, contudo, muitas vezes desconhecemos sua origem. Refletindo sobre esse fato, sua segunda tarefa consiste em deduzir a expressão popularmente conhecida no Brasil como "fórmula de Bháskara", partindo de uma equação polinomial de 2º grau na forma $ax^2+bx+c=0$, onde $a \neq 0$.

Estude os dois temas propostos e organize um texto apresentando as respostas para as questões destacadas, além da dedução para a fórmula de resolução das equações de 2º grau em sua forma geral. Construa também uma breve apresentação para que vocês possam compartilhar seus estudos e reflexões com os demais colegas do grupo de estudos, propondo uma discussão a respeito da importância do professor em conhecer as deduções para as fórmulas empregadas nas resoluções de equações polinomiais considerando o trabalho com essas expressões na educação básica, de modo a favorecer a compreensão dos alunos sobre o tema.

Não pode faltar

Na educação básica, o estudo dos polinômios tem início nos últimos anos do ensino fundamental e pode ser associado, inclusive, a outros campos da Matemática, como a Geometria. Podemos empregar os polinômios no estudo do perímetro, área e volume de figuras geométricas como forma de apresentar uma aplicação desse conceito em problemas práticos. No entanto, para que o professor possa estabelecer essas associações, é necessário, inicialmente, que ele aprofunde seus estudos no tema em questão, conhecendo a definição e as principais propriedades e operações associadas ao conjunto de polinômios.

Polinômios sobre anéis

Considere um anel $(A,+,\cdot)$ comutativo com unidade. Um **polinômio** na variável x com coeficientes no conjunto A é uma soma da forma $a_0+a_1x+a_2x^2+a_3x^3+\ldots+a_nx^n+\ldots$, onde cada $a_i \in A$, para todo $i \in \mathbb{N}$, tal que $a_k=0$ para todo $k>n$, com $n \in \mathbb{N}$. Os escalares $a_i \in A$ são chamados de **coeficientes** do polinômio. Como todos os coeficientes do polinômio são

nulos a partir de a_{n+1}, podemos denotar o polinômio na forma $f(x)=a_0+a_1x+a_2x^2+a_3x^3+...+a_nx^n$. Por exemplo, podemos representar o polinômio $1-3x+4x^2+0x^3+0x^4+...$ como $1-3x+4x^2$ ou $f(x)=1-3x+4x^2$. O coeficiente a_n do termo x^n, que corresponde à potência de *x* com maior expoente, é chamado de **coeficiente líder** ou **coeficiente dominante** de *f*. Por exemplo, o polinômio $p(x)=2-3x^2+5x^4$ tem coeficiente dominante como sendo o termo $a_4=5$, ou seja, o coeficiente do termo x^4, a qual corresponde à potência de *x* com maior expoente. E em particular, quando o coeficiente dominante de um polinômio for igual a 1, podemos dizer que o polinômio é **mônico**. O polinômio $q(x)=2x^2+x^3$, por exemplo, tem como coeficiente dominante o termo $a_3=1$, fazendo com que o polinômio $q(x)$ seja mônico.

Assimile

Podemos ainda associar os polinômios com sequências definidas sobre um anel comutativo com unidade $(A,+,\cdot)$. Um polinômio pode ser definido como uma sequência $(a_0, a_1, a_2, a_3, ..., a_n, ...)$ em que todos os termos $a_i \in A$ para todo $i \in \mathbb{N}$, tal que $a_k=0$ para todo $k>n$, sendo $n \in \mathbb{N}$ algum índice. Nessa representação, o polinômio $1-3x+4x^2+0x^3+0x^4+...$ pode ser descrito na forma $(1,-3, 4, 0, 0, ..., 0, ...)$.

O anel $(A,+,\cdot)$ que possibilita a estruturação dos polinômios pode ser tomado, por exemplo, como o anel dos inteiros $(\mathbb{Z},+,\cdot)$, o qual goza das propriedades que definem os anéis comutativos com unidade. Podemos ainda considerar como base os anéis $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$, $(\mathbb{Z}_m,+,\cdot)$ com *m* primo, entre outros, desde que se trate de um anel comutativo com unidade.

Considerando a definição de polinômio, podemos definir uma **função polinomial** sobre *A* como uma função $f: A \to A$ dada por $f(x)=a_0+a_1x+a_2x^2+a_3x^3+...+a_nx^n$. É possível considerar essa representação como uma **forma padrão** para a função polinomial, na qual os expoentes da variável *x* são considerados em ordem crescente. Note que podemos ordenar as funções polinomiais

em ordem decrescente, sendo que nesse caso não teremos a representação em sua forma padrão. Para os estudos que serão realizados, consideraremos a expressão polinômio sobre *A* com o mesmo significado de "função polinomial sobre *A*".

Com base no conjunto de polinômios, podemos estudar exemplos importantes e propriedades, como os graus e algumas classificações.

Um exemplo de polinômio é o **nulo**, que corresponde àquele cujos coeficientes são todos nulos e que pode ser representado como $0(x) = 0 + 0x + 0x^2 + 0x^3 + \ldots$, ou na forma da sequência nula $(0, 0, 0, \ldots, 0, \ldots)$. Outro polinômio importante é o **constante**, que corresponde ao polinômio na forma $f(x) = a$ para todo $x \in A$, ou na forma de sequência, como $(a, 0, \ldots, 0, \ldots)$. Nesse caso, temos o polinômio constante determinado por *a*.

Considere um polinômio $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n$ não nulo, com $a_n \neq 0$ e $n \geq 0$ natural, definido sobre um anel $(A, +, \cdot)$ comutativo com unidade. Nesse caso, dizemos que o polinômio $f(x)$ tem grau *n*, o qual pode ser denotado por $grau(f) = n$. Por exemplo, o polinômio $p(x) = 2 - 3x^2 + 5x^4$ é tal que $grau(p) = 4$, enquanto o polinômio $q(x) = 2x^2 + x^3$ é tal que $grau(q) = 3$.

Reflita

Vimos que a definição de grau toma por base um polinômio não nulo. É possível estudar o grau associado a um polinômio nulo? Qual a relação existente entre o polinômio nulo e a presença de coeficiente dominante?

Considere os polinômios $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ e $g(x) = b_0 + b_1x + b_2x^2 + \ldots + b_nx^n$ definidos sobre um anel $(A, +, \cdot)$ comutativo com unidade. Diremos que os polinômios $f(x)$ e $g(x)$ serão iguais quando os polinômios forem de mesmo grau e quando $a_k = b_k$ para todos os valores de *k*, com *k* natural, isto é, os coeficientes dos termos de mesmo grau forem iguais. Considerando o conjunto $\mathbb{Z}[x]$ dos polinômios com coeficientes inteiros, veja, por exemplo, que os polinômios $r(x) = 1 - x^2 + x^3$ e $s(x) = 1 + 0x - x^2 + x^3$ são iguais, porque são de mesmo grau e os

coeficientes dos termos correspondentes são iguais. Por outro lado, note que $t(x)=2-x^2+3x^3$ e $w(x)=2-x+3x^2$ não são iguais, visto que não são de mesmo grau, também, $y(x)=1-2x^2$ e $z(x)=1+2x^2$ não são iguais, pois os coeficientes do termo x^2 são diferentes.

Faça você mesmo

Determine que condições devem ser satisfeitas pelos números reais *a*, *b* e *c* para que os polinômios $f(x)=(a-2)x^2-bx+c$ e $g(x)=4x^2-5bx-3c$ sejam iguais.

Agora, vamos estudar raízes e valores de um polinômio. Para isso, considere um anel comutativo com unidade $(A,+,\cdot)$, sobre o qual é construído o polinômio $f(x)=a_0+a_1x+a_2x^2+\ldots+a_nx^n$. Dado um escalar $\beta\in A$, dizemos que $f(\beta)=a_0+a_1\beta+a_2\beta^2+\ldots+a_n\beta^n$ é o **valor** de *f* em β. Sendo *A* um anel, que é fechado em relação à $+$ e $\cdot$ em *A*, $f(\beta)=a_0+a_1\beta+a_2\beta^2+\ldots+a_n\beta^n\in A$. Quando $f(\beta)=0$, dizemos que β é **raiz** de *f* em *A*.

Considere, por exemplo, o polinômio $f(x)=2-3x^2+x^4\in\mathbb{Z}[x]$. O valor de *f* em -2 é $f(-2)=2-3(-2)^2+(-2)^4=2-12+16=6$. Note que $f(1)=2-3\cdot1^2+1^4=2-3+1=0$, logo, 1 é raiz de *f*. Observe agora o polinômio $g(x)=1+x^2\in\mathbb{R}[x]$. Note que $x^2\geq0$ para todo $x\in\mathbb{R}$, então $1+x^2\geq1>0$ para todo $x\in\mathbb{R}$. Dessa forma, não existe nenhum número real *x* para o qual $1+x^2=0$. Isso quer dizer que $g(x)=1+x^2$ não admite raízes reais em $\mathbb{R}$. Assim, no estudo das raízes de polinômios é imprescindível indicar em qual conjunto o polinômio possui ou não raiz, porque, apesar de $g(x)=1+x^2$ não admitir raiz em $\mathbb{R}$, esse mesmo polinômio admite raiz em $\mathbb{C}$.

Observamos até o momento a possibilidade de construir um conjunto de polinômios $A[x]$ a partir de um anel comutativo com unidade $(A,+,\cdot)$. Será que podemos construir um anel com base em um conjunto de polinômios? Vejamos na sequência como podemos construir operações de modo a compor um anel com base em um conjunto de polinômios.

Anéis de polinômios

Considere um anel $(A,+,\cdot)$ comutativo com unidade. O conjunto dos polinômios sobre o anel A é

$$A[x] = \{\text{polinômios na variável } x \text{ com coeficientes em } A\}$$
$$= \left\{a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \middle| a_i \in A,\ i \in \mathbb{N},\ \text{e } n \in \mathbb{N}\right\}$$

Dados $f(x),\ g(x) \in A[x]$, digamos $f(x) = a_0 + a_1x + \ldots + a_nx^n$ e $g(x) = b_0 + b_1x + \ldots + b_mx^m$ com $m \leq n$, podemos definir as seguintes operações:

- **Adição** em $A[x]$: $f(x) + g(x) = c_0 + c_1x + \ldots + c_nx^n$ com $c_k = a_k + b_k$ para todos $k = 0,1,2,\ldots,n$ e sendo $b_k = 0$ para todo $k > m$.

- **Multiplicação** em $A[x]$: $f(x)g(x) = c_0 + c_1x + \ldots + c_{m+n}x^{m+n}$ com os coeficientes c_k dados por:

$$c_0 = a_0b_0,\quad c_1 = a_0b_1 + a_1b_0,\quad c_2 = a_0b_2 + a_1b_1 + a_2b_0,\quad \ldots,$$
$$c_k = a_0b_k + a_1b_{k-1} + a_2b_{k-2} + \cdots + a_{k-1}b_1 + a_kb_0 = \sum_{i=0}^{k} a_ib_{k-i}$$

com $i \in \mathbb{N}$, para todo $k \leq m+n$, sendo $b_k = 0$ para todo $k > m$ e $a_k = 0$ para todo $k > n$.

Assimile

Note que a adição de polinômios consiste em somar os coeficientes correspondentes dos polinômios envolvidos, ou seja, somar os coeficientes associados às potências de x de mesmo grau. Quando multiplicamos dois polinômios entre si, precisamos somar os produtos envolvendo cada um dos termos do primeiro polinômio com cada um dos termos do segundo, aplicando a distributividade da multiplicação em relação à adição, propriedade verificada no anel $(A,+,\cdot)$.

Com base no conjunto apresentado e nas operações definidas anteriormente, podemos estudar o seguinte resultado:

Proposição 4: $(A[x],+,\cdot)$ pode ser classificado como anel, denominado **anel de polinômios**.

Demonstração: Para verificar que $(A[x],+,\cdot)$ é um anel, precisamos mostrar que $(A[x],+,\cdot)$ é um grupo abeliano, que $(A[x],\cdot)$ goza do fechamento e associatividade, e que em $(A[x],+,\cdot)$

vale a distributividade da multiplicação em relação à adição. Em relação ao estudo de $(A[x],+)$, nos limitaremos a estudar os elementos neutro e simétrico. Por isso, estude e comprove a validade do fechamento e da associatividade em $(A[x],+)$. Note que o elemento neutro de $(A[x],+)$ corresponde ao polinômio nulo $0(x)$ estudado anteriormente, pois $0(x)+f(x)=f(x)+0(x)=f(x)$ para todo $f(x)\in A[x]$. Além disso, todo $f(x)=a_0+a_1x+\ldots+a_nx^n\in A[x]$ admite um elemento simétrico $-f(x)=-a_0-a_1x+\ldots-a_nx^n$, tal que $f(x)+[-f(x)]=[-f(x)]+f(x)=0(x)$. Logo, $(A[x],+)$ é um grupo abeliano. De modo análogo ao do estudo de $(A[x],+)$, podemos verificar que $(A[x],\cdot)$ goza do fechamento e associatividade, considerando a multiplicação de polinômios conforme definição anterior, por isso, verifique a validade de cada uma dessas afirmações com base no que foi estudado a respeito da estrutura de anel e considerando as definições das operações de adição e multiplicação de polinômios. Além disso, temos a distributividade da multiplicação em relação à adição sendo válida em $(A[x],+,\cdot)$.

Note que se $(A,+,\cdot)$ é um anel comutativo com unidade, a estrutura $(A[x],+,\cdot)$ pode ser classificada como um anel, conforme estudado na Proposição 4. Além disso, $(A[x],+,\cdot)$ é um anel comutativo com unidade, porque a multiplicação de polinômios é comutativa e, além disso, admite o elemento neutro, ou a unidade, como sendo o polinômio $u(x)=1=1+0x+0x^2+\ldots$. Portanto, se $(A,+,\cdot)$ é um anel comutativo com unidade, então o anel de polinômios $(A[x],+,\cdot)$ é comutativo com unidade, sendo seu zero o polinômio nulo $0(x)=0$ e sua unidade o polinômio $u(x)=1$.

Faça você mesmo

Mostre que o conjunto *A* está contido em $A[x]$ com base nas definições dos polinômios constantes de $A[x]$.

No entanto, veja que $(A[x],+,\cdot)$ não pode ser classificado como corpo. De fato, seja, nesse anel, o polinômio $f(x)=x$ não nulo. Se $f(x)$ fosse inversível, existiria $g(x)=b+b_1x+\ldots+b_mx^m$, com b_m não nulo, tal que $f(x)g(x)=x\cdot(b_0+b_1x+\ldots+b_mx^m)=1=u(x)$ para todo $x\in A$. Assim, em particular, para o zero do anel $(A,+,\cdot)$ ($x=0$),

teríamos $f(0)=0$ e, nesse caso, $0=f(0)\cdot g(0)=u(0)=1$, o que não é possível, porque $0\neq 1$. Portanto, existem polinômios não nulos em $(A[x],+,\cdot)$ que não são inversíveis, logo $(A[x],+,\cdot)$ não pode ser classificado como corpo.

Reflita

Considere o anel $(A[x],+,\cdot)$ comutativo com unidade. Levando em conta dois polinômios $f(x)$ e $g(x)$ definidos sobre A, o que podemos dizer a respeito do grau do polinômio $f(x)+g(x)$? E do grau de $f(x)g(x)$?

Vimos que se $(A,+,\cdot)$ é um anel comutativo com unidade, então o anel de polinômios $(A[x],+,\cdot)$ é comutativo com unidade. No entanto, além das operações de adição e multiplicação de polinômios, podemos ainda definir a divisão de polinômios, a qual é estruturada a partir do seguinte algoritmo:

Proposição 5 (algoritmo da divisão de polinômios): Sejam $(A,+,\cdot)$ um corpo, $f(x)$ e $g(x)$ polinômios de $(A[x],+,\cdot)$, com $g(x)$ não nulo. Então existem polinômios $q(x),r(x)\in A[x]$, tais que $f(x)=g(x)q(x)+r(x)$ com $grau(r(x))<grau(g(x))$, ou $r(x)=0$, sendo $q(x)$ e $r(x)$ são os únicos polinômios que satisfazem a essa igualdade.

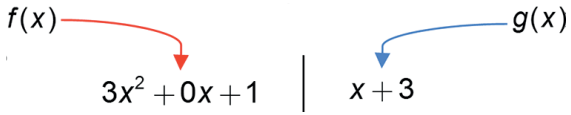
Para a demonstração desse resultado, consulte as páginas 21 e 22 de Koerich (2000).

Podemos associar o algoritmo da divisão de polinômios com a divisão de inteiros e ao dividir $f(x)$ (dividendo) por $g(x)$ (divisor), buscamos a identificação de um quociente $q(x)$ e de um resto $r(x)$ sujeito às condições apresentadas no Teorema 2. Vejamos agora a aplicação do **método das chaves** para a identificação do quociente e do resto da divisão de polinômios.

Exemplificando

Considere os polinômios $f(x)=3x^2+1$ e $g(x)=x+3$, ambos representados na ordem decrescente de seus termos. Note que $f(x)$ pode ser reescrito como $f(x)=3x^2+0x+1$. Para aplicar o método das chaves, vamos construir a representação da Figura 4.5.

Figura 4.5 | Representação do método das chaves



Fonte: elaborada pela autora.

Note que a representação é semelhante à da divisão de inteiros. Vamos iniciar o processo dividindo o termo $3x^2$ de $f(x)$ pelo termo x de $g(x)$, o que resulta em $3x$, termo que será incluído abaixo da chave que contém $g(x)$, conforme a Figura 4.6. Vamos agora multiplicar $3x$ por $g(x)$ e acrescentar o resultado desse produto abaixo do polinômio $f(x)$, efetuando uma subtração, conforme indicado na Figura 4.6.

Figura 4.6 | Primeira etapa da divisão de $f(x)$ por $g(x)$

$$\begin{array}{r|l} 3x^2+0x+1 & x+3 \\ \cline{2-2} -\ 3x^2+9x & 3x \\ \cline{1-1} \quad -9x+1 & \end{array}$$

Fonte: elaborada pela autora.

Dividindo $-9x$ por x (os primeiros termos do resultado da subtração e de $g(x)$, respectivamente), obtemos o resultado -9, o qual devemos adicionar ao termo abaixo da chave. Em seguida, multiplicamos -9 por $g(x)$ e indicamos o resultado abaixo de $-9x+1$, efetuando uma subtração, conforme observamos na Figura 4.7.

Figura 4.7 | Segunda etapa da divisão de $f(x)$ por $g(x)$

$$\begin{array}{r|l} 3x^2+0x+1 & x+3 \\ \cline{2-2} -\ 3x^2+9x & 3x-9 \\ \cline{1-1} \quad -9x+1 & \\ -\ -9x-27 & \\ \cline{1-1} \quad\quad 28 & \end{array}$$

Fonte: elaborada pela autora.

Como o grau de $r(x)=28$ é menor que o grau de $g(x)$, podemos encerrar o método e concluir que ao dividir $f(x)=3x^2+1$ por $g(x)=x+3$, temos que o quociente da divisão é $q(x)=3x-9$ e o resto, $r(x)=28$.

Note que no exemplo apresentado, o resto da divisão é 28, que é um valor não nulo. Quando $r(x)=0$, podemos concluir que a **divisão** do polinômio $f(x)$ por $g(x)$ é **exata**.

Pesquise mais

Para complementar os estudos a respeito da divisão de polinômios, consulte o capítulo 3 do material indicado a seguir. Nele, além do método das chaves, é apresentado um outro método para a divisão de polinômios: o dispositivo de Briot-Ruffini, bem como as demais operações envolvendo polinômios, podendo ser empregado como um material complementar a respeito dos polinômios.

MENDES, Gabriel; ALMEIDA, Thaís de; OLIVEIRA, Lucas. **Polinômios**. Disponível em: <http://www2.ime.unicamp.br//~ma225/2014Tarefa4-GrupoBtxt.pdf>. Acesso em: 25 out. 2018.

Em relação aos polinômios, um dos principais temas a ser estudado, consiste na identificação das raízes e, nesse sentido, podemos estudar diferentes resultados que tratam a respeito desse conteúdo, dentre os quais podemos destacar o Teorema Fundamental da Álgebra.

Raízes de polinômios

Considere um anel comutativo com unidade $(A,+,\cdot)$ e um polinômio $p(x)\in A[x]$.

Proposição 6: Se $(A,+,\cdot)$ for um anel de integridade e $p(x)\in A[x]$ for não nulo, então o número de raízes de $p(x)$ é menor ou igual ao grau de $p(x)$.

Ou seja, pela Proposição 6, a quantidade de raízes de um polinômio é limitada por seu grau, de modo que um polinômio de grau *n* pode ter no máximo *n* raízes.

Outro resultado que possibilita a avaliação das raízes de um polinômio em $\mathbb{C}[x]$ é o seguinte:

Proposição 7 (Teorema Fundamental da Álgebra): Todo polinômio $p(x)\in\mathbb{C}[x]$ com grau maior ou igual a 1 admite ao menos uma raiz complexa, ou seja, existe $z\in\mathbb{C}$, tal que $p(z)=0$.

Além do Teorema Fundamental da Álgebra, temos outros dois resultados que possibilitam a investigação das raízes de polinômios em $\mathbb{C}[x]$.

Proposição 8: Se um polinômio complexo $p(x)$ com coeficientes reais admite $z \in \mathbb{C}$ como raiz, então o conjugado de z, representado por $\bar{z}$, é também raiz de $p(x)$.

Proposição 9: Se um polinômio complexo $p(x)$ com coeficientes reais apresenta grau ímpar, então $p(x)$ admite ao menos uma raiz real.

Desses resultados podemos, por exemplo, concluir que polinômios de grau 1 sempre admitem uma raiz real, enquanto polinômios de grau 2 podem apresentar duas raízes complexas conjugadas, duas raízes reais distintas ou uma raiz real de multiplicidade 2, que são as possibilidades estudadas desde a Educação Básica para os polinômios com coeficientes reais.

O conhecimento desses resultados pode favorecer na organização dos trabalhos com polinômios desde a educação básica, porque, além de fundamentarem esse campo de conhecimentos, permitem ao professor a identificação dos exemplos e tarefas mais adequadas a seus objetivos.

Pesquise mais

Para complementar os estudos sobre polinômios, consulte o trecho entre as páginas 45 e 51 da dissertação *O Teorema Fundamental da Álgebra*. Disponível em: https://sca.profmat-sbm.org.br/sca_v2/get_tcc3.php?id=94490. Acesso em: 13 set. 2018.

Leia também as páginas 31 e 40 do trabalho de conclusão de curso intitulado *Um estudo sobre polinômios e sua abordagem no ensino*, de Aline C. Koerich. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/94973/Aline_Casagrande_Koerch.PDF?sequence=1. Acesso em: 13 set. 2018.

Sem medo de errar

Retomando a proposta do grupo de estudos para o segundo encontro, você e outros dois colegas ficaram responsáveis por apresentar aos demais professores os resultados de estudos relativos ao conjunto de polinômios, sendo o primeiro tema voltado

à associação dos polinômios com a estrutura de corpo e o segundo à dedução da fórmula empregada na resolução de equações polinomiais de 2º grau, ou na identificação das raízes de polinômios de grau 2.

Para a primeira tarefa, vocês devem analisar as vantagens em construir polinômios com base em corpos em vez de apenas anéis.

Conforme estudado anteriormente, um corpo $(A,+,\cdot)$ corresponde a um anel no qual a segunda operação binária goza da comutatividade, existência de elemento neutro e existência de elemento simétrico a todo elemento não nulo. Logo, todo corpo é um anel, mas nem todo anel é um corpo.

Quando construímos um anel de polinômios sobre um corpo, podemos verificar a presença de outras propriedades além daquelas que seriam observadas se a estrutura inicial fosse apenas um anel.

Podemos estabelecer as seguintes relações entre anéis e anéis de polinômios:

- Se $(A,+,\cdot)$ é um anel, então $(A[x],+,\cdot)$ é um anel, em que $A[x]$ corresponde ao conjunto dos polinômios na variável x com coeficientes pertencentes ao conjunto A.
- Se $(A,+,\cdot)$ é um anel comutativo, então $(A[x],+,\cdot)$ é um anel comutativo.
- Se $(A,+,\cdot)$ é um anel com unidade, então $(A[x],+,\cdot)$ é um anel com unidade.
- Se $(A,+,\cdot)$ é um domínio de integridade, então $(A[x],+,\cdot)$ é um domínio de integridade.
- Se $(A,+,\cdot)$ é um corpo, então $(A[x],+,\cdot)$ é um domínio de integridade.

Essas relações podem ser comprovadas pelas relações entre os polinômios, seus coeficientes e o tipo de estrutura que está sendo considerada para sua construção.

Logo, quando a estrutura $(A,+,\cdot)$ for um corpo, o anel de polinômios $(A[x],+,\cdot)$ poderá ser classificado como um domínio de integridade, ou seja, além de ser um anel, sua multiplicação gozará da comutatividade e existência de elemento neutro, além de ser verificada a lei do anulamento do produto. No entanto, assim como estudado, mesmo que $(A,+,\cdot)$ seja um corpo, não teremos que $(A[x],+,\cdot)$ será um corpo, porque existem polinômios não

nulos de $A[x]$ que não são inversíveis. Dessa forma, a vantagem em construir anéis de polinômios com base em corpos se dá pelo fato de verificarmos propriedades adicionais relativas à operação de multiplicação de polinômios.

A segunda tarefa consiste em deduzir a fórmula empregada para a resolução de equações polinomiais de grau 2, ou seja, em identificar a fórmula utilizada na identificação das raízes de um polinômio. Para isso, considere a expressão $ax^2+bx+c=0$, na qual *a*, *b* e *c* são números reais e que $a\neq 0$. Multiplicando ambos membros da igualdade considerada por $4a$, obtemos $(4a)(ax^2+bx+c)=(4a)0=0$, o que pela propriedade distributiva da multiplicação em relação à adição implica em $4a^2x^2+4abx+4ac=0$.

Adicionando o elemento oposto a $4ac$ nos dois lados da igualdade anterior, segue pela associatividade e existência de elemento neutro da adição que $(4a^2x^2+4abx+4ac)+(-4ac)=0+(-4ac)=-4ac$, ou ainda, $4a^2x^2+4abx=-4ac$.

Ao adicionar o termo b^2 em ambos os membros da última igualdade obtida, e empregando a comutatividade, temos $4a^2x^2+4abx+b^2=-4ac+b^2=b^2-4ac$.

Como $(2ax+b)^2=4a^2x^2+4abx+b^2$, da última igualdade segue que $(2ax+b)^2=b^2-4ac$, o que por meio da radiciação implica $\sqrt{(2ax+b)^2}=\sqrt{b^2-4ac}$. Como $\sqrt{x^2}=|x|$, para todo *x* real da igualdade obtida anteriormente, teremos $2ax+b=\pm\sqrt{b^2-4ac}$.

Adicionando o oposto a *b* em ambos os membros da última igualdade, e pela associatividade, comutatividade e existência de elemento neutro da adição segue com o $2ax=-b\pm\sqrt{b^2-4ac}$.

Multiplicando os membros da última igualdade pelo inverso de $2a$, que existe porque $2a$ é um número real não nulo, segue pela associatividade e existência de elemento neutro da multiplicação que $\left(\frac{1}{2a}\right)(2ax)=\left(\frac{1}{2a}\right)\left(-b\pm\sqrt{b^2-4ac}\right)$, ou ainda, $x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$

que corresponde à fórmula para identificação das raízes de um polinômio na forma $p(x)=ax^2+bx+c$ com *a*, *b* e *c* números reais, com *a* não nulo.

Para finalizar, elabore uma apresentação aos demais docentes integrantes do grupo que evidencie os principais tópicos estudados

por você e seus colegas nas duas tarefas desenvolvidas. Elabore um documento com as principais explicações a respeito dos conceitos envolvidos de modo a auxiliá-lo no momento da apresentação e das discussões com os demais integrantes do grupo de estudos.

Avançando na prática

Polinômios definidos sobre conjuntos na forma $\mathbb{Z}_p$, com p natural

Descrição da situação-problema

Imagine que você atua como professor de Matemática em uma escola da educação básica e pretende elaborar uma atividade que envolva a operação de multiplicação de polinômios, estudando os graus dos polinômios envolvidos. Você observou que ao multiplicar um polinômio $f(x)$ de grau 2 por um polinômio $g(x)$ de grau 3, ambos com coeficientes reais, foi obtido como resultado um polinômio $f(x)g(x)$ de grau 5 com coeficientes reais. Assim, no caso analisado, temos que $grau(f)+grau(g)=grau(fg)$. No entanto, essa expressão é válida para anéis de polinômios definidos sobre qualquer anel $(A,+,\cdot)$? Investigue a relação apresentada no anel $(\mathbb{Z}_4[x],+,\cdot)$ e verifique se a mesma continua sendo válida. Que condição deve ser satisfeita por $(A,+,\cdot)$ para que o anel de polinômios $(A[x],+,\cdot)$ goze da relação $grau(f)+grau(g)=grau(fg)$ para todos $f(x),g(x)\in A[x]$? De que forma essa condição pode contribuir no estudo de polinômios na educação básica?

Resolução da situação-problema

Queremos investigar a relação $grau(f)+grau(g)=grau(fg)$ no anel de polinômios $(\mathbb{Z}_4[x],+,\cdot)$, definido sobre o anel dos inteiros módulo 4. Para isso, sejam dois polinômios em $\mathbb{Z}_4[x]$ como $f(x)=\bar{1}+\bar{2}x$ e $g(x)=\bar{2}x$, note que ambos os polinômios são de grau 1. Sendo assim, $grau(f)+grau(g)=1+1=2$. Como $(\mathbb{Z}_4,+,\cdot)$ é um anel, então $(\mathbb{Z}_4[x],+,\cdot)$ também goza da estrutura de anel. Assim, segue das propriedades de um anel que

$$f(x)g(x)=\left(\bar{1}+\bar{2}x\right)\left(\bar{2}x\right)=\bar{1}\cdot\left(\bar{2}x\right)+\bar{2}x\cdot\left(\bar{2}x\right)=\bar{2}x+\bar{4}x^2=\bar{2}x+\bar{0}x^2=\bar{2}x$$

ou seja, $f(x)g(x)=\bar{2}x$ corresponde a um polinômio de grau 1, logo $grau(fg)=1$. Portanto, $grau(f)+grau(g)=2\neq 1=grau(fg)$, isto é, a relação não é válida em $(\mathbb{Z}_4[x],+,\cdot)$. Essa conclusão se deve ao

fato de $(\mathbb{Z}_4,+,\cdot)$ não ser um domínio de integridade, ou seja, de possuir divisores de zero, o que implica na relação não ser válida no caso indicado e para nenhum outro anel de polinômios que seja construído a partir de um anel $(A,+,\cdot)$ que não seja classificado como domínio de integridade. Como o anel $(\mathbb{R},+,\cdot)$ é um corpo e, consequentemente, um domínio de integridade, temos que o anel de polinômios $(\mathbb{R}[x],+,\cdot)$ será um domínio de integridade, o que implica no fato de, nessa estrutura, ser válida a relação $grau(f)+grau(g)=grau(fg)$ para todos $f(x),g(x)\in\mathbb{R}[x]$. Assim, o conhecimento dessa condição pode contribuir na reflexão e na compreensão da multiplicação entre polinômios com coeficientes reais. De que forma o professor pode empregar essa relação para contribuir com o aprendizado dos alunos a respeito da operação de multiplicação entre polinômios com coeficientes reais? Reflita a respeito dessa questão e finalize a elaboração do plano de aula com a seleção de um problema relativo à multiplicação de polinômios com base no estudo realizado a respeito da condição envolvendo os graus dos polinômios.

Faça valer a pena

1. Podemos classificar os polinômios de acordo com as características de seus monômios, ou seja, de cada um dos produtos envolvendo um coeficiente e uma potência da variável em questão.

No estudo dos polinômios, podemos nos deparar com os polinômios completos, que são aqueles que apresentam todos os monômios desde o coeficiente constante até o termo com a potência de maior expoente, coincidente com seu grau, para a variável em estudo.

Considerando essa categoria e as demais classificações, associe os polinômios (indicados por I, II, III e IV) com suas respectivas classificações (denotadas por A, B, C e D):

$$\text{I. } p(x)=3-x+x^2+2x^3$$

$$\text{II. } q(x)=3+3x$$

$$\text{III. } r(x)=-1+2x+x^2$$

$$\text{IV. } s(x)=9-4x^2$$

A. Polinômio mônico
B. Polinômio de grau 3.
C. Polinômio incompleto.
D. Polinômio de grau 1.

Assinale a alternativa que indica todas as associações corretamente:

a) I – A; II – B; III – D; IV – C.
b) I – B; II – D; III – A; IV – C.
c) I – D; II – B; III – C; IV – A.
d) I – C; II – A; III – D; IV – B.
e) I – B; II – A; III – C; IV – D.

2. Ao empregar o algoritmo euclidiano para a divisão de polinômios, visamos a decomposição de um polinômio $f(x)$ em função de outros três polinômios, $g(x)$, $q(x)$ e $r(x)$, de modo que $f(x)=g(x)q(x)+r(x)$.
Com base nesse tema, considere um polinômio $f(x)=x^5+ax^4+bx^2+cx+1\in\mathbb{R}[x]$. Sabemos que ao dividir o polinômio $f(x)$ por $d_1(x)=x-1$, obtém-se resto $r_1(x)=2$. Por outro lado, quando dividimos $f(x)$ por $d_2(x)=x+1$, o resto obtido é $r_2(x)=3$.

Sabendo que o polinômio $f(x)$ é divisível por $d_3(x)=x-2$, ou seja, a divisão de $f(x)$ por $d_3(x)$ é exata, assinale a alternativa que indica corretamente a expressão que caracteriza o polinômio $f(x)$:

a) $f(x)=x^5-3x^4+\frac{9}{2}x^2-\frac{3}{2}x+1$.
b) $f(x)=x^5-x^4+4x^2-2x+1$.
c) $f(x)=x^5-x^4+\frac{1}{2}x+1$.
d) $f(x)=x^5-2x^2+5x+1$.
e) $f(x)=x^5+3x^4+8x^2-5x+1$.

3. Considerando os polinômios e suas propriedades, analise as seguintes afirmações:
I. O polinômio $f(x)=(a+b-5)x^2+(b+c-7)x+(a+c)$ será identicamente nulo se, e somente se, $a=-1$, $b=6$ e $c=1$.
II. Os polinômios $g(x)=2ax^2+bx+c$ e $h(x)=(a+1)x^2+2bx-c$ serão iguais somente quando $a=-1$, $b=0$ e $c=0$.
III. O polinômio $p(x)=x^4-3ax^3+(2a-b)x^2+2bx+(a+3b)$ será divisível por $q(x)=x^2-3x+4$ apenas quando $a=1$ e $b=-3$.
IV. Ao dividirmos o polinômio $f(x)=x^4-3x^3+6x^2$ por $g(x)=x^2-3x+5$, obtemos o quociente $q(x)=x^2+1$ e resto $r(x)=3x-5$.

Em relação às afirmações apresentadas, assinale a alternativa correta.

a) Apenas as afirmações I e II estão corretas.
b) Apenas as afirmações I e IV estão corretas.
c) Apenas as afirmações II e III estão corretas.
d) Apenas as afirmações II e IV estão corretas.
e) As afirmações I, III e IV estão corretas.

Seção 4.3

Homomorfismos, isomorfismos e domínios euclidianos

Diálogo aberto

Nas seções anteriores estudamos os anéis e suas propriedades, observando que eles podem ser construídos a partir de diferentes conjuntos, como os numéricos, de funções, de matrizes, de polinômios, entre outros. No caso da segunda operação binária, que caracteriza o anel gozar de outras propriedades, além das que estão presentes na definição, temos ainda subcategorias a serem avaliadas.

Um dos conteúdos abordados na educação básica são as funções de uma variável real com suas propriedades, inclusive com a avaliação das leis de formação, domínios e contradomínios. Diante desse conceito, seria possível identificar uma forma semelhante a essa para comparar diferentes estruturas entre si, além do conjunto de números reais? Podemos construir aplicações cujos domínios e contradomínios correspondam a anéis? Assim, mediante esses questionamentos, nesta seção estudaremos os homomorfismos e isomorfismos de anéis, bem como os domínios euclidianos, visando investigar a possibilidade de associação entre anéis e as contribuições desses estudos para a identificação de propriedades presentes nessas estruturas.

Assim, dando sequência às reflexões a respeito de tópicos da álgebra, no terceiro encontro do grupo de estudos, a proposta é o estudo dos homomorfismos e isomorfismos de anéis, relacionando-os com o conceito de função, importante tema abordado na educação básica.

Diante disso, você deverá estudar e elaborar uma apresentação para os demais integrantes do grupo a respeito dos homomorfismos e isomorfismos de anéis, associando com o conceito de função. Para tanto, você pretende iniciar uma discussão com os colegas a respeito dos seguintes questionamentos: como podemos relacionar as funções de uma variável real com os conceitos de homomorfismos e isomorfismos de anéis? Quais são as semelhanças e as diferenças entre esses conceitos? Como o conhecimento dos homomorfismos

e isomorfismos contribui com o ensino das funções de uma variável real na educação básica?

A fim de contribuir com o estudo do tema proposto, você decidiu apresentar um exemplo de aplicação entre anéis, partindo dos seguintes conjuntos:

$$M = \left\{a + b\sqrt{-2};\ a, b \in \mathbb{Q}\right\} \text{ e } \quad N = M_2(\mathbb{Q}) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix};\ a, b, c, d \in \mathbb{Q}\right\}$$

munidos, respectivamente, das operações usuais de adição e multiplicação de números racionais e de matrizes quadradas de ordem 2 com entradas reais, compondo os anéis $(M, +, \cdot)$ e $(N, +, \cdot)$. Com base nesses conjuntos, foi definida a aplicação $f : M \to N$, dada por $f(a + b\sqrt{-2}) = \begin{pmatrix} a & -2b \\ b & a \end{pmatrix}$. Assim, para apresentar essa aplicação aos colegas, primeiramente você deve estudá-la, verificando se *f* pode ser classificada como homomorfismo ou isomorfismo de anéis, justificando a resposta com base nos conceitos teóricos.

Que conceitos são necessários para a resolução das tarefas propostas? Construa um texto e uma apresentação contemplando o tema em questão, considerando as definições dos homomorfismos e isomorfismos de anéis e a análise do exemplo selecionado.

Para a finalização desse desafio, de posse das resoluções construídas ao longo da unidade, você poderá elaborar seu portfólio, essencial para a conclusão dessa fase do grupo de estudos. Assim, organize todas as atividades desenvolvidas ao longo dos três encontros e construa seu portfólio, acrescentando as reflexões a respeito das contribuições dos estudos realizados no grupo de estudos para o trabalho com os conteúdos matemáticos abordados na educação básica.

Não pode faltar

Nas seções anteriores estudamos a estrutura de anel e suas principais subcategorias, como os anéis comutativos com unidade, os domínios de integridade e os corpos. Com base nas propriedades presentes em cada estrutura podemos identificar as mais adequadas para a resolução de problemas, como os que envolvem equações polinomiais, por exemplo.

Nesta seção pretendemos organizar os anéis em classes de modo a identificar propriedades que caracterizam cada uma delas.

Considerando os conceitos estudados pela área da geometria plana, sabemos que é possível organizar figuras geométricas em grupos a partir do conceito de congruência, de tal forma que, ao construir determinado conjunto de triângulos congruentes, por exemplo, conseguimos deduzir propriedades para todas as figuras do conjunto a partir do estudo de um de seus representantes. Assim, nosso objetivo é, de modo análogo ao caso da congruência, estudar as classes de anéis que apresentam as mesmas características, a menos de notação, por meio dos conceitos de homomorfismos e isomorfismos de anéis, a fim de construir correspondências biunívocas entre anéis de uma mesma classe.

Homomorfismos de anéis

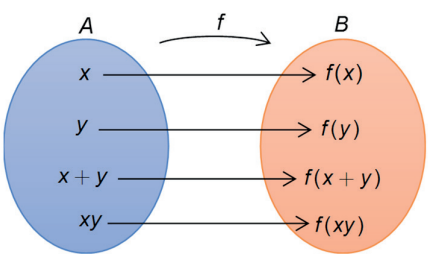
Um **homomorfismo** do anel $(A, \oplus, \otimes)$ em um anel $(B, \Delta, *)$ é uma aplicação $f : A \to B$ que satisfaz, para quaisquer $x, y \in A$, as seguintes condições: $f(x \oplus y) = f(x) \Delta f(y)$ e $f(x \otimes y) = f(x) * f(y)$.

Assimile

Note que as operações presentes no 1º membro das duas igualdades anteriores correspondem às operações definidas sobre o anel $(A, \oplus, \otimes)$, já as operações presentes no 2º membro são referentes ao anel $(B, \Delta, *)$.

Para simplificar as correspondências, vamos nos referir a $f : A \to B$ como um homomorfismo de anéis, o qual pode ser representado na forma de diagramas como o da Figura 4.8, e, quando se tratar de um mesmo anel, sendo $A = B$, f será chamado de homomorfismo de A.

Figura 4.8 | Homomorfismo do anel $(A, \oplus, \otimes)$ no anel $(B, \Delta, *)$



Fonte: elaborada pela autora.

Note que em um homomorfismo podemos associar diferentes anéis entre si, em que cada um apresenta suas operações características, as quais não precisam ser iguais para os dois anéis.

No entanto, para simplificar a notação, prosseguiremos os nossos estudos adotando os símbolos $+$ e $\cdot$ para representar duas operações binárias quaisquer definidas sobre um conjunto. Dessa forma, quando denotarmos dois anéis quaisquer por $(A,+,\cdot)$ e $(B,+,\cdot)$, apesar das notações iguais, as operações definidas sobre esses anéis não necessariamente serão iguais.

Exemplificando

Considere os anéis $(A,+,\cdot)$ e $(B,+,\cdot)$, bem como a aplicação $f: A \to B$ definida por $f(x) = e_B$, onde e_B é o elemento neutro da adição em B, para todo $x \in A$. Note que f é um homomorfismo de anéis, denominado **homomorfismo nulo**, pois dados $x, y \in A$ temos que $f(x+y) = e_B = e_B + e_B = f(x) + f(y)$ e $f(x \cdot y) = e_B = e_B \cdot e_B = f(x) \cdot f(y)$. Logo, f é um homomorfismo do anel $(A,+,\cdot)$ em $(B,+,\cdot)$.

Outro exemplo que podemos destacar corresponde a considerar um anel $(A,+,\cdot)$ e definir uma aplicação $g: A \to A$ dada por $g(x) = x$ para todo $x \in A$. A aplicação g é um homomorfismo sobre A, denominado **homomorfismo identidade**, pois para $x, y \in A$ segue que $f(x+y) = x + y = f(x) + f(y)$ e $f(x \cdot y) = x \cdot y = f(x) \cdot f(y)$. Portanto, g é um homomorfismo sobre o anel $(A,+,\cdot)$.

Considere o anel dos inteiros $(\mathbb{Z},+,\cdot)$ e definamos a aplicação $h: \mathbb{Z} \to \mathbb{Z}$ por $h(x) = -x$ para todo x inteiro. Note que h não é um homomorfismo, visto que, para os inteiros 1 e 2, temos $h(1 \cdot 2) = h(2) = -2$ e $h(1)h(2) = (-1)(-2) = 2$, logo, $h(1 \cdot 2) \neq h(1)h(2)$. Dessa forma, h não é um homomorfismo sobre $\mathbb{Z}$.

Quando desejamos provar que uma aplicação é um homomorfismo de anéis, devemos comprovar a validade das duas condições presentes na definição para todos os elementos do domínio da aplicação. No entanto, se desejamos mostrar

que uma aplicação não é homomorfismo, basta apresentarmos um contraexemplo para uma das condições que caracterizam a definição.

Faça você mesmo

Sejam os anéis $(\mathbb{Z},+,\cdot)$ e $(\mathbb{Z}\times\mathbb{Z},+,\cdot)$ (produto direto), defina a aplicação $f:\mathbb{Z}\to\mathbb{Z}\times\mathbb{Z}$ por $f(x)=(x,0)$. A aplicação *f* é um homomorfismo de $\mathbb{Z}$ em $\mathbb{Z}\times\mathbb{Z}$? Justifique sua resposta.

Quando um homomorfismo $f:A\to B$ entre os anéis $(A,+,\cdot)$ e $(B,+,\cdot)$ for tal que se $x\neq y$, então $f(x)\neq f(y)$ para todos $x,y\in A$, logo, diremos que *f* é um **homomorfismo injetor**. Além disso, se o homomorfismo *f* é tal que dado $y\in B$ qualquer, sempre podemos determinar $x\in A$, tal que $f(x)=y$, diremos que *f* é um **homomorfismo sobrejetor**. E no caso de *f* ser um homomorfismo injetor e sobrejetor simultaneamente, diremos que *f* é um **homomorfismo bijetor**.

Podemos estudar propriedades associadas aos homomorfismos de acordo com as características do anel ou dos anéis envolvidos, conforme a seguinte proposição.

Proposição 10: Seja $f:A\to B$ um homomorfismo do anel $(A,+,\cdot)$ no anel $(B,+,\cdot)$, então:

(a) $f(e_A)=e_B$, onde e_A e e_B são os elementos neutros de $+$ relativos aos anéis $(A,+,\cdot)$ e $(B,+,\cdot)$, respectivamente.

(b) $f(-x)=-f(x)$ para todo $x\in A$.

(c) Se *f* é um homomorfismo sobrejetor e $(A,+,\cdot)$ é um anel com unidade, com 1_A sendo sua unidade, então $(B,+,\cdot)$ será um anel com unidade, admitindo a unidade $f(1_A)$.

Demonstração: (a) Aplicando *f* sobre a expressão $e_A=e_A+e_A$, teremos $f(e_A)=f(e_A+e_A)$, e por *f* ser homomorfismo, $f(e_A)=f(e_A)+f(e_A)$. Logo, $2f(e_A)-f(e_A)=e_B$, e assim, $f(e_A)=e_B$.

(b) Seja $x\in A$. Aplicando *f* sobre $x+(-x)=e_A$, que pode ser avaliada porque $(A,+,\cdot)$ é um anel, obtemos $f(x+(-x))=f(e_A)$. Por se tratar de um homomorfismo e sendo válida a propriedade descrita em (a), segue que $f(x)+f(-x)=f(e_A)=e_B$. Adicionando $-f(x)$ a ambos os

membros da última igualdade tem-se $[-f(x)]+f(x)+f(-x)=[-f(x)]+e_B$, isto é, $f(-x)=-f(x)$.

(c) Considere $y \in B$, como f é um homomorfismo sobrejetor, existe $x \in A$ tal que $f(x)=y$. Dessa forma, $y \cdot f(1_A)=f(x)\cdot f(1_A)=f(x\cdot 1_A)=f(x)=y$ e $f(1_A)\cdot y=f(1_A)\cdot f(x)=f(1_A\cdot x)=f(x)=y$, isto é, $f(1_A)$ corresponde à unidade de $(B,+,\cdot)$, o que permite classificá-lo como anel com unidade.

Reflita

Considerando as hipóteses presentes na proposição 10, relativas à existência de um homomorfismo do anel $(A,+,\cdot)$ no anel $(B,+,\cdot)$, se $(A,+,\cdot)$ for um anel comutativo, o que podemos afirmar a respeito da presença da comutatividade da operação $\cdot$ no anel $(B,+,\cdot)$?

A partir desse teorema, podemos observar que ao associar anéis entre si a partir de um homomorfismo, algumas propriedades podem ser identificadas em ambas as estruturas, desde que determinadas hipóteses sejam verificadas.

Seja $f: A \to B$ um homomorfismo entre os anéis $(A,+,\cdot)$ e $(B,+,\cdot)$. Dessa aplicação podemos estudar um subconjunto importante de A, chamado de núcleo. O **núcleo do homomorfismo** f, denotado por $N(f)$ ou $\ker(f)$, corresponde ao seguinte subconjunto: $N(f)=\{x \in A \mid f(x)=e_B\}$. Esse conjunto é não vazio, porque ao menos $e_A \in N(f)$, já que $f(e_A)=e_B$ de acordo com a proposição 10. Com o núcleo de um homomorfismo podemos estudar a injetividade do homomorfismo.

Proposição 11: Considere $f: A \to B$ um homomorfismo entre os anéis $(A,+,\cdot)$ e $(B,+,\cdot)$. Dessa forma, f é um homomorfismo injetor se, e somente se, $N(f)=\{e_A\}$.

Demonstração: Se f é injetor e como $f(e_A)=e_B$, pela proposição 10, temos que $N(f)=\{e_A\}$. Por outro lado, se $N(f)=\{e_A\}$ e $f(x)=f(y)$ para $x,y \in A$, ou $f(x)-f(y)=e_B$, pelo item (b) da proposição 10, temos $f(x)+f(-y)=e_B$, e, sendo f um homomorfismo, $f(x-y)=e_B$, o que implica em $x-y \in N(f)$, assim, $x-y=e_A$, ou $x=y$, comprovando a injetividade de f.

Pela proposição 11 temos condições de avaliar a injetividade de um homomorfismo a partir de seu núcleo. Por exemplo, o núcleo do homomorfismo nulo corresponde a $N(f) = A$, o que permite afirmar que o homomorfismo nulo não é injetivo. O homomorfismo identidade é tal que apenas $g(e_A) = e_A$, então $N(g) = \{e_A\}$, fazendo com que o homomorfismo identidade seja injetor.

O estudo dos homomorfismos é importante para a comprovação da validade de determinadas afirmações relativas à Teoria dos Números. Vejamos no próximo exemplo como o conhecimento dos homomorfismos favorece a construção e validação do critério de divisibilidade de um número inteiro por 9, tomando por base o conjunto dos números inteiros $\mathbb{Z}$ e o conjunto das classes de resto módulo 9, denotado por $\mathbb{Z}_9$, e que está associado aos restos da divisão de inteiros por 9.

Exemplificando

Sabemos que um número inteiro *n* é divisível por 9 quando a soma dos algarismos de *n* for um número divisível por 9. Vamos comprovar essa afirmação com base no conceito de homomorfismo.

Seja o homomorfismo $\phi : \mathbb{Z} \to \mathbb{Z}_9$ dado por $\phi(x) = \overline{a}$, em que *a* corresponde ao resto da divisão de *x* por 9, ou podemos ainda empregar o conceito de módulo e representar $a \equiv x (\text{mod } 9)$, logo, $\phi(x) = x (\text{mod } 9)$. Por exemplo, se $x = 12$, então ao dividirmos *x* por 9 obtemos quociente 1 e resto 3, porque $12 = 9 \cdot 1 + 3$, então, $\phi(12) = \overline{3}$. Como sugestão de estudo, prove que essa aplicação ϕ corresponde a um homomorfismo de anéis.

Para provar o critério de divisibilidade dos inteiros por 9, considere que um número inteiro *n* admita a representação $a_k a_{k-1} \ldots a_1 a_0$, na qual os algarismos a_i são tais que $0 \leq a_i \leq 9$ para todo $i = 0, 1, 2, \ldots, k$ e $a_k \neq 0$. Assim, o número *n* pode ser dado como $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0$.

Note que o inteiro *n* será divisível por 9 se, e somente se, $\phi(n) = \overline{0}$, isto é, se o resto da divisão de *n* por 9 for igual a 0. Veja que, pela representação de *n*, é válida a seguinte igualdade:

$$\phi(n) = \phi(a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0)$$
$$= \overline{a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0}$$

Considerando as operações definidas sobre $\mathbb{Z}_9$ e sabendo que $\phi(10) = \bar{1}$, porque o resto da divisão de 10 por 9 é igual a 1, segue que:

$$\begin{aligned}\phi(n) &= \overline{a_k}\,\overline{10}^k + \overline{a_{k-1}}\,\overline{10}^{k-1} + \ldots + \overline{a_1}\,\overline{10} + \overline{a_0} \\ &= \overline{a_k}\,\bar{1}^k + \overline{a_{k-1}}\,\bar{1}^{k-1} + \ldots + \overline{a_1}\,\bar{1} + \overline{a_0} \\ &= \overline{a_k} + \overline{a_{k-1}} + \ldots + \overline{a_1} + \overline{a_0} \\ &= \overline{a_k + a_{k-1} + \ldots + a_1 + a_0}\end{aligned}$$

Portanto, *n* será divisível por *9* quando $\overline{a_k + a_{k-1} + \ldots + a_1 + a_0} = \bar{0}$, isto é, se $a_k + a_{k-1} + \ldots + a_1 + a_0$ (a soma dos algarismos que compõem o número *n*) for divisível por 9.

Vejamos outro exemplo de homomorfismo de anéis. Considere o anel dos reais $(\mathbb{R}, +, \cdot)$ e o anel de matrizes $(A, +, \cdot)$, em que $A = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in M_2(\mathbb{R}) \right\}$. Vamos definir a aplicação $f : \mathbb{R} \to A$ por $f(x) = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$, para todo *x* real. Note que, para todos $x, y \in \mathbb{R}$,

$$f(x+y) = \begin{pmatrix} x+y & 0 \\ 0 & x+y \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} + \begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix} = f(x) + f(y)$$

$$f(xy) = \begin{pmatrix} xy & 0 \\ 0 & xy \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}\begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix} = f(x)f(y)$$

Sendo assim, *f* é um homomorfismo de $\mathbb{R}$ em *A*. Em relação a esse homomorfismo, podemos ainda verificar que, dados $x, y \in \mathbb{R}$ com $f(x) = f(y)$, então $\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} = \begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix}$, o que implica em $x = y$, logo, *f* é injetivo. Além disso, dada qualquer $X = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in A$, existe $a \in \mathbb{R}$, pois as entradas de *X* são números reais, de modo que $f(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = X$, isto é, *f* pode ser classificado como sobrejetivo.

Dessa forma, *f* é um homomorfismo injetivo e sobrejetivo, ou seja, *f* é um homomorfimo bijetor. Devido a essa propriedade, podemos dizer que *f* é um isomorfismo de $\mathbb{R}$ em *A* e, assim, temos uma categoria particular de homomorfismos.

Isomorfismos de anéis

Seja $f : A \to B$ um homomorfismo de anéis, se *f* for também bijetor, então *f* será chamado de **isomorfismo** do anel $(A,+,\cdot)$ no anel $(B,+,\cdot)$. Neste caso, dizemos que *f* é um isomorfismo de anéis e que os anéis $(A,+,\cdot)$ e $(B,+,\cdot)$ são isomorfos.

Por exemplo, o homomorfismo identidade $g : A \to A$ dado por $g(x) = x$, para todo $x \in A$, com $(A,+,\cdot)$ anel, é bijetor, por isso *g* é um isomorfismo sobre *A*.

Sendo $\mathbb{Z}\left[\sqrt{3}\right] = \left\{ a + b\sqrt{3} \mid a,b \in \mathbb{Z} \right\}$, temos que $f : A \to A$ definida por $f\left(a + b\sqrt{3}\right) = a - b\sqrt{3}$ é um isomorfismo. De fato, para $x = a + b\sqrt{3},\ y = c + d\sqrt{3} \in \mathbb{Z}\left[\sqrt{3}\right]$ segue que

$$f(x+y) = (a+c) - (b+d)\sqrt{3} = \left(a - b\sqrt{3}\right) + \left(c - d\sqrt{3}\right) = f(x) + f(y)$$

$$f(xy) = (ac + 3bd) - (ad + bc)\sqrt{3} = \left(a - b\sqrt{3}\right)\left(c - d\sqrt{3}\right) = f(x)f(y)$$

Assim, *f* é um homomorfismo. Como $N(f) = \{0\}$, temos que *f* é injetor pela proposição 11. Além disso, dado $y = a + b\sqrt{3} \in \mathbb{Z}\left[\sqrt{3}\right]$, basta tomar $x = a - b\sqrt{3} \in \mathbb{Z}\left[\sqrt{3}\right]$ e, assim, $f(x) = y$, ou seja, *f* é sobrejetor. Como *f* é um homomorfismo bijetor, podemos concluir que *f* é um isomorfismo.

Considere o anel dos inteiros $(\mathbb{Z},+,\cdot)$. Conforme estudado anteriormente, esse anel pode ser classificado como um domínio de integridade. Além disso, podemos estudar, sobre esse anel, o algoritmo da divisão derivado das operações usuais de adição e multiplicação. O anel dos inteiros pode ser associado a outros por meio de homomorfismos ou isomorfismos, o que indica a existência de características semelhantes entre os anéis envolvidos. Sendo assim, existem outras estruturas nas quais podem ser definidos algoritmos de divisão, semelhante àquele presente em $(\mathbb{Z},+,\cdot)$? No tópico seguinte vamos estudar estruturas que apresentam essa propriedade e que são chamadas de domínios euclidianos.

Domínios euclidianos

Considere $(D,+,\cdot)$ um domínio de integridade. Sendo e_D o elemento neutro da operação $+$ definida sobre D, vamos construir uma função $\varphi : D-\{e_D\} \to \mathbb{N}$ de tal forma que:

(i) $\varphi(x) \leq \varphi(xy)$ para todos $x, y \in D-\{e_D\}$

(ii) Se $x, y \in D$, $y \neq e_D$, existem $q, r \in D$ com $x = yq + r$ e tal que $r = e_D$ ou $\varphi(r) < \varphi(y)$

Se as condições (i) e (ii) são válidas para φ, então $(D,+,\cdot,\varphi)$ é um **domínio euclidiano**.

Assimile

Note que o domínio euclidiano envolve a generalização do algoritmo da divisão, característico dos inteiros, para domínios de integridade em geral.

O anel dos inteiros $(\mathbb{Z},+,\cdot)$ é um domínio de integridade. Além disso, considerando a função $\varphi : \mathbb{Z}-\{0\} \to \mathbb{N}$ dada por $\varphi(x) = |x|$ para todo x inteiro não nulo, ou seja, φ está associada ao cálculo do valor absoluto dos inteiros não nulos x, temos que $(\mathbb{Z},+,\cdot,\varphi)$ pode ser classificado como um domínio euclidiano, pois temos $|x| \leq |xy|$ para todos $x, y \in \mathbb{Z}^*$, o que implica na validade da condição (i), e é válido o algoritmo da divisão em $\mathbb{Z}^*$, relacionado à condição (ii).

Podemos também construir domínios euclidianos a partir de anéis de polinômios, tema estudado na seção anterior.

Exemplificando

Considere $(K,+,\cdot)$ um corpo a partir do qual podemos construir o anel de polinômios $(K[x],+,\cdot)$. Este anel de polinômios, associado à função

$$\begin{aligned} \varphi : K[x]-\{0\} &\to \mathbb{N} \\ f &\mapsto \varphi(f) = grau(f) \end{aligned}$$

compõe um domínio euclidiano, em que $grau(f)$ denota o grau do polinômio f, associado ao expoente da variável presente no termo dominante de f.

De fato, vamos comprovar as duas condições presentes na definição. Se f e g são polinômios não nulos, então $grau(fg) = grau(f) + grau(g)$.

Assim, para $f,g \in K[x]-\{0\}$, ou seja, f e g são não nulos, temos $\varphi(f)=grau(f)>0$ e $\varphi(g)=grau(g)>0$. Desse modo, $\varphi(f)<\varphi(f)+\varphi(g)=\varphi(fg)$, o que garante que $\varphi(f)\leq\varphi(fg)$ e comprova a condição (i). A condição (ii) está associada ao algoritmo da divisão de polinômios, estudado a partir da proposição 5 apresentada na seção anterior. Dessa forma, como $(K,+,\cdot)$ é um corpo, ao considerar $f,g \in K[x]$, com g não nulo, é possível identificar polinômios $q,r \in K[x]$ de modo que, para todo $x \in K$, $f(x)=g(x)q(x)+r(x)$ com $r=0$ ou $\varphi(r)<\varphi(g)$, comprovando a validade de (ii). Portanto, $(K[x],+,\cdot,\varphi)$ pode ser classificado como domínio euclidiano.

O estudo dos domínios euclidianos contribui para a identificação de estruturas nas quais podemos identificar algoritmos de divisão correspondentes. Assim, temos a composição de estruturas em que podemos identificar duas operações, uma "adição" e uma "multiplicação", além do estudo de uma "subtração", interpretada como a "adição" com o oposto, e uma "divisão", relativa ao algoritmo da divisão derivado das operações de "adição" e "multiplicação", possibilitando uma associação com as quatro operações básicas estudadas a partir do conjunto de números reais e seus principais subconjuntos.

Dessa forma, a partir desses estudos, o professor pode identificar a fundamentação teórica para as quatro operações básicas sobre os números reais e suas respectivas técnicas de cálculo, abordadas na educação básica, construindo propostas que favoreçam as aprendizagens dos alunos em relação a esses conteúdos e demais tópicos associados.

Pesquise mais

Para complementar os estudos a respeito de homomorfismos e isomorfismos de anéis, consulte o capítulo 2 do material Álgebra II, no trecho entre as páginas 16 e 19 e entre as páginas 22 e 28. Disponível em: <https://canalcederj.cecierj.edu.br/012016/501d58b01832672a6f395366b2abe406.pdf>. Acesso em: 14 set. 2018.

Verifique os exercícios resolvidos e as partes das proposições que dizem respeito às definições de homomorfismos e isomorfismos.

Sem medo de errar

No contexto de participação do terceiro encontro do grupo de estudos, você ficou responsável por elaborar uma apresentação para os demais integrantes que contemple uma discussão sobre a importância do conhecimento dos homomorfismos e isomorfismos de anéis para a formação do professor, bem como a associação desses conceitos com as funções de uma variável real, conteúdo abordado na educação básica e o estudo de uma aplicação entre anéis específica, justificando se corresponde a um homomorfismo e/ou isomorfismo de anéis.

Quando estudamos as funções de uma variável real, identificamos três elementos básicos: o domínio, o contradomínio e a lei de formação, sendo que, nesse caso em específico, o domínio e o contradomínio correspondem a subconjuntos de $\mathbb{R}$. Devido às operações usuais de adição e multiplicação definidas sobre $\mathbb{R}$, e que podem ser restritas a seus subconjuntos, podemos investigar as funções cujas leis de formação dependem de forma direta, ou indireta, das propriedades relativas a essas operações, estudando as aplicações relativas ao corpo $(\mathbb{R},+,\cdot)$ ou aos seus subanéis. No caso das funções em que o domínio e o contradomínio correspondem a todo o $\mathbb{R}$, por exemplo, temos aplicações sobre o anel dos reais. Assim, podemos relacionar as funções reais à definição de homomorfismo e observar que existem casos específicos de funções que podem ser caracterizadas como homomorfismos, enquanto outras não apresentam essa característica.

Por exemplo, considere a função $f:\mathbb{R}\to\mathbb{R}$ definida por $f(x)=x+1$. Note que $f(2)=3$ e $f(3)=4$, porém, $f(2+3)=f(5)=6\neq 3+4=f(2)+f(3)$ e $f(2\cdot 3)=f(6)=7\neq 12=f(2)\cdot f(3)$. Logo, *f* é uma aplicação do anel $(\mathbb{R},+,\cdot)$ em $(\mathbb{R},+,\cdot)$ que não satisfaz as condições presentes na definição de homomorfismo, logo, *f* não é um homomorfismo sobre $(\mathbb{R},+,\cdot)$. Por outro lado, sendo $g:\mathbb{R}\to\mathbb{R}$ dada por $g(x)=x$, podemos identificar que $g(x+y)=x+y=g(x)+g(y)$ e $g(xy)=xy=g(x)g(y)$ para todos *x* e *y* reais, o que possibilita a caracterização de *g* como homomorfismo.

Dessa forma, podemos observar que os homomorfismos em que o domínio e o contradomínio correspondem a $\mathbb{R}$, munido de suas operações de adição e multiplicação usuais, consistem em funções reais que satisfazem a definição de homomorfismo. Mas

note que nem toda função é um homomorfismo de anéis, mas todos os homomorfismos cujos anéis envolvidos são $(\mathbb{R},+,\cdot)$ ou seus subanéis correspondem a funções reais.

No caso dos isomorfismos, temos uma situação análoga, considerando agora o fato de que as funções envolvidas devem ser bijetivas e apresentarem as condições presentes na definição de homomorfismo. Assim, um exemplo que podemos destacar é a função *g* descrita anteriormente, cuja lei de formação é $g(x)=x$ para todo *x* real, a qual é uma função bijetiva e um homomorfismo, o que implica *g* ser um isomorfismo.

Para concluir este estudo, reflita sobre as contribuições do conhecimento dos homomorfismos e isomorfismos para a formação do professor que, no exercício de sua profissão, poderá deparar-se com situações em que precisará trabalhar com conceitos, como é o caso das funções, que estão relacionadas aos homomorfismos e isomorfismos. Elabore outros questionamentos que podem contribuir com a realização da discussão que deverá ser conduzida por você no grupo de estudos, a respeito desse tema.

Como forma de aprofundar os conhecimentos a respeito dos homomorfismos e isomorfismos de anéis, o qual foi identificado como contribuição importante para a formação do professor, você pretende discutir, durante sua apresentação, a respeito da possibilidade de classificação de determinada aplicação como homomorfismo ou isomorfismo de anéis. Para esse estudo, sejam os conjuntos

$$M=\left\{a+b\sqrt{-2};\ a,b\in\mathbb{Q}\right\} \quad \text{e} \quad N=M_2(\mathbb{Q})=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix};\ a,b,c,d\in\mathbb{Q}\right\}$$

e a aplicação $f:M\to N$ definida por

$$f(a+b\sqrt{-2})=\begin{pmatrix}a & -2b\\ b & a\end{pmatrix}$$

Considerando $x=a+b\sqrt{-2}$ e $y=c+d\sqrt{-2}$, elementos quaisquer do conjunto *M*, segue que

$$f(x+y)=f\left((a+c)+(b+d)\sqrt{-2}\right)=\begin{pmatrix}a+c & -2(b+d)\\ b+d & a+c\end{pmatrix}=\begin{pmatrix}a+c & -2b-2d\\ b+d & a+c\end{pmatrix}$$

$$=\begin{pmatrix}a & -2b\\ b & a\end{pmatrix}+\begin{pmatrix}c & -2d\\ d & c\end{pmatrix}=f\left(a+b\sqrt{-2}\right)+f\left(c+d\sqrt{-2}\right)=f(x)+f(y)$$

$$f(xy)=f\left((ac-2bd)+(ad+bc)\sqrt{-2}\right)=\begin{pmatrix}ac-2bd & -2(ad+bc)\\ ad+bc & ac-2bd\end{pmatrix}=\begin{pmatrix}ac-2bd & -2ad-2bc\\ ad+bc & ac-2bd\end{pmatrix}$$

$$= \begin{pmatrix} a & -2b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} c & -2d \\ d & c \end{pmatrix} = f\left(a + b\sqrt{-2}\right) f\left(c + d\sqrt{-2}\right) = f(x)f(y)$$

Logo, *f* é um homomorfismo do anel $(M, +, \cdot)$ no anel $(N, +, \cdot)$. Para verificar se *f* é um isomorfismo, temos que analisar se *f* é injetor e sobrejetor. Dados $x = a + b\sqrt{-2}$ e $y = c + d\sqrt{-2}$ pertencentes a *M*, de modo que $f(x) = f(y)$, ou $f(x) = \begin{pmatrix} a & -2b \\ b & a \end{pmatrix} = \begin{pmatrix} c & -2d \\ d & c \end{pmatrix} = f(y)$, então $a = c$ e $b = d$, isto é, $x = y$, o que implica em *f* ser injetor. No entanto, considerando a matriz $A = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \in N$, veja que não existe nenhum elemento pertencente a *M* cuja imagem seja a matriz *A*, logo, *f* não é sobrejetor. Portanto, *f* é um homomorfismo injetor que não é sobrejetor, assim, *f* não é um isomorfismo de anéis.

Elabore um texto contendo todas as observações realizadas ao longo dos estudos e elabore uma apresentação para os demais colegas a respeito do tema proposto. Procure elencar questionamentos e dúvidas que podem ser abordadas durante as discussões como forma de aprofundar os estudos sobre o tema, considerando também a aplicação *f* selecionada para contribuir com os estudos a respeito dos homomorfismos e isomorfismos de anéis.

Finalizando a proposta de estudo dos três encontros do grupo referentes à Álgebra, conclua a elaboração do portfólio acrescentando todas as atividades que foram desenvolvidas ao longo dos encontros, procurando acrescentar as reflexões sobre quais as contribuições dos estudos dos temas propostos pelo grupo para a formação do professor e para o trabalho com os conteúdos matemáticos na educação básica.

Avançando na prática

Forma polar ou trigonométrica para os números complexos na educação básica

Descrição da situação-problema

Suponha que você, como professor de Matemática de uma turma de Ensino Médio, pretende elaborar um plano de aula voltado ao estudo da forma polar dos números complexos e optou

por tarefas que envolvam o anel dos inteiros de Gauss $(Z[i],+,\cdot)$, $\mathbb{Z}[i]=\{a+bi \mid a,b\in\mathbb{Z}\}$, de modo a simplificar os cálculos e a identificação das representações geométricas, pois a proposta é que os alunos utilizem papel milimetrado nesse estudo. Para a forma polar de um número $z=a+bi$, é necessário calcular o seu módulo, dentre outros, o qual pode ser interpretado geometricamente. Tomando a função $\varphi:\mathbb{Z}[i]-\{0\}\to\mathbb{N}$ dada por $\varphi(a+bi)=a^2+b^2$, relativa ao módulo de *z*, $(Z[i],+,\cdot,\varphi)$ pode ser classificado como um domínio euclidiano? De que forma essa caracterização contribui com o estudo da divisão e da forma polar de números complexos, de acordo com a abordagem realizada nos livros didáticos de Matemática para o ensino médio?

Resolução da situação-problema

Note que $(Z[i],+,\cdot,\varphi)$ é um domínio euclidiano. De fato, considere $x=a+bi,\ y=c+di\in\mathbb{Z}[i]$, ambos não nulos. Sendo assim,

$$\varphi(xy)=\varphi((ac-bd)+(ad+bc)i)=(ac-bd)^2+(ad+bc)^2$$
$$=a^2c^2+a^2d^2+b^2c^2+b^2d^2=\left(a^2+b^2\right)\left(c^2+d^2\right)=\varphi(x)\varphi(y)$$

Como $a^2+b^2\geq 0$, $c^2+d^2\geq 0$, então $\varphi(xy)=\varphi(x)\varphi(y)\geq\varphi(x)$, comprovando a condição (i) da definição. Para a condição (ii), sejam $x=a+bi,\ y=c+di\in\mathbb{Z}[i]$, *y* não nulo. Sendo $\overline{y}$ o conjugado do número complexo *y*, ao calcularmos a divisão de *x* por *y*, devemos multiplicar e dividir o termo $\frac{x}{y}$ por $\overline{y}$, obtendo uma fração cujo numerador é $x\overline{y}$ e denominador é $y\overline{y}$, sendo este último termo dado por $y\overline{y}=\varphi(y)$. Assim, note que

$$xy^{-1}=\frac{x}{y}=\frac{x\overline{y}}{y\overline{y}}=\frac{x\overline{y}}{\varphi(y)}=\frac{(a+bi)(c-di)}{c^2+d^2}=\frac{ac+bd}{c^2+d^2}+\frac{bc-ad}{c^2+d^2}i=m+ni\in\mathbb{Q}[i]$$

Em cada intervalo da forma $(c,c+1)$, com $c\in\mathbb{Q}$, existe um número inteiro. Veja a demonstração desse resultado na página 14 do material de Sousa (2013). Assim, tomando na afirmação anterior $c=-\frac{1}{2}$, podemos identificar *r* e *s* inteiros, tais que $|m-r|\leq\frac{1}{2}$ e $|n-s|\leq\frac{1}{2}$, com $m=\frac{ac+bd}{c^2+d^2}$ e $n=\frac{bc-ad}{c^2+d^2}$. Assim, note que

$$xy^{-1} = m + ni = (r - r + m) + (s - s + n)i = (r + si) + \left[(m - r) + (n - s)i\right]$$
$$\Rightarrow \quad x = (r + si)y + \left[(m - r) + (n - s)i\right]y$$

Considerando $q = r + si$ e $r = \left[(m - r) + (n - s)i\right]y$, sabendo que $y = c + di$, segue que

$$\varphi(r) = \varphi\left(\left[(m - r) + (n - s)i\right]y\right) = \varphi\left((m - r) + (n - s)i\right)\varphi(y) \leq \left(\frac{1}{4} + \frac{1}{4}\right)\varphi(y) < \varphi(y)$$

comprovando a decomposição de *x* na forma $x = yq + r$, com $r = 0$ ou $\varphi(r) < \varphi(y)$ e a condição (ii) desejada.

Considerando a elaboração de uma proposta voltada ao trabalho com a forma polar, e também com as operações envolvendo números complexos, de que forma a caracterização de $(Z[i], +, \cdot, \varphi)$ como domínio euclidiano favorece a elaboração das tarefas? Por que o anel dos inteiros de Gauss pode contribuir com a aprendizagem dos números complexos no ensino médio? Finalize a tarefa identificando atividades que poderiam ser selecionadas com base nesse anel, para o estudo do módulo de um número complexo e sua forma polar.

Faça valer a pena

1. Para a definição de um homomorfismo, precisamos considerar dois anéis, os quais podem ser iguais entre si, além de uma aplicação definida entre eles, de modo que satisfaça a duas condições para todos os elementos do anel, caracterizando o domínio da aplicação. Dessa forma, é necessário que todas as condições da definição sejam válidas simultaneamente para afirmar que a aplicação definida corresponde a um homomorfismo de anéis.
Com base nesse tema, considere as aplicações definidas a seguir:

$$f : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z} \text{ definida por } f(x) = (0, x)$$
$$g : \mathbb{Z} \to \mathbb{Z} \text{ definida por } g(x) = 3x + 2$$
$$h : \mathbb{C} \to \mathbb{C} \text{ definida por } h(a + bi) = a - bi$$

Além disso, considere que os anéis $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ (produto direto) e $(\mathbb{C}, +, \cdot)$ estejam munidos de suas operações usuais de adição e multiplicação.

Considerando as aplicações apresentadas, assinale a alternativa que indica a(s) que pode(m) ser classificada(s) como homomorfismo(s) de anéis:

a) Apenas *f*.
b) Apenas *f* e *g*.
c) Apenas *f* e *h*.
d) Apenas *g* e *h*.
e) As aplicações *f*, *g* e *h*.

2. A partir da caracterização de um homomorfismo, podemos estudar algumas de suas propriedades específicas. Além disso, podemos identificar um subconjunto de seu domínio formado por todos os elementos, cujas imagens são nulas, compondo o chamado núcleo do homomorfismo. Considere os homomorfismos definidos como segue:

$$f : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z} \text{ definido por } f(x,y) = x$$
$$g : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}\times\mathbb{Z} \text{ definido por } g(x,y) = (y,x)$$
$$h : \mathbb{Z} \to \mathbb{Z}\times\mathbb{Z} \text{ definido por } h(x) = (0,-x)$$

A respeito dos homomorfismos apresentados, assinale a alternativa correta:
a) O núcleo do homomorfismo *f* corresponde a $N(f) = \{(0,0)\}$.
b) O núcleo do homomorfismo *g* corresponde a $N(g) = \mathbb{R}$.
c) O núcleo do homomorfismo *h* corresponde a $N(h) = \{(0,x) \mid x \in \mathbb{Z}\}$.
d) O núcleo do homomorfismo *f* corresponde a $N(f) = \{(0,y) \mid y \in \mathbb{Z}\}$.
e) O núcleo do homomorfismo *g* corresponde a $N(g) = \{0\}$.

3. Considerando as definições dos homomorfismos e dos isomorfismos, bem como de suas principais propriedades, analise as afirmações apresentadas a seguir, classificando-as como verdadeiras (V) ou falsas (F):
( )Todo homomorfismo na forma $f : A \to B$, em que $(A,+,\cdot)$ e $(B,+,\cdot)$ são anéis com unidade, satisfazem à condição de que $f(1_A) = 1_B$, com 1_A e 1_B representando, respectivamente, as unidades dos anéis $(A,+,\cdot)$ e $(B,+,\cdot)$.
( )A aplicação $f : \mathbb{Q}\times\mathbb{Z} \to \mathbb{Z}\times\mathbb{Q}$ definida por $f(x,y) = (y,x)$ pode ser classificada como um isomorfismo de anéis.
( )Os anéis $(2\mathbb{Z},+,\cdot)$ e $(3\mathbb{Z},+,\cdot)$, munidos de suas operações usuais de adição e multiplicação, são isomorfos, ou seja, é possível construir um isomorfismo $f : 2\mathbb{Z} \to 3\mathbb{Z}$.

Assinale a alternativa que apresenta a sequência correta das classificações, considerando a ordem na qual as afirmações foram apresentadas:
a) V – F – V.
b) V – F – F.
c) F – V – V.
d) F – F – V.
e) F – V – F.

Referências

BEDOYA, Hernando; CAMELIER, Ricardo. **Álgebra II**. Rio de Janeiro: Fundação CECIERJ, 2010.

COCHMANSKI, Julio Cesar; COCHMANSKI, Liliane Cristina de Camargo. **Estruturas algébricas**. Curitiba: InterSaberes, 2016.

DIAS, Fábio Campos. **O Teorema fundamental da álgebra**. 2017. 6 f. Dissertação (Mestrado Profissional em Matemática) – Universidade Federal do Amapá, Macapá. Disponível em: <https://sca.profmat-sbm.org.br/sca_v2/get_tcc3.php?id=94490>. Acesso em: 13 set. 2018.

DOMINGUES, Hygino H.; IEZZI, Gelson. Álgebra moderna. São Paulo: Atual, 2003.

GARCIA, Arnaldo; LEQUAIN, Yves. **Elementos de álgebra**. Rio de janeiro: IMPA, 2015.

HEFEZ, Abramo. **Curso de álgebra**. Rio de Janeiro: IMPA, 2014. 1 v.

JANESCH, Oscar Ricardo; TANEJA, Inder Jeet. Álgebra I. 2 ed. Florianópolis: UFSC/EAD/CED/CFM, 2011. Disponível em: <http://mtm.grad.ufsc.br/files/2014/04/%C3%81lgebra-I.pdf>. Acesso em: 13 set. 2018.

KOERICH, Aline Casagrande. **Um Estudo sobre Polinômios e sua abordagem no Ensino**. 2000. 76 f.Trabalho de Conclusão de Curso (Licenciatura em Matemática) – Universidade Federal de Santa Catarina, Florianópolis. Disponível em: <https://repositorio.ufsc.br/bitstream/handle/123456789/94973/Aline_Casagrande_Koerch.PDF?sequence=1>. Acesso em: 13 set. 2018.

LEITE, Álvaro Emílio; CASTANHEIRA, Nelson Pereira. **Teoria dos números e teoria dos conjuntos**. Curitiba: InterSaberes, 2014.

MENDES, Gabriel; ALMEIDA, Thaís de; OLIVEIRA, Lucas. **Polinômios**. Disponível em: <http://www2.ime.unicamp.br//~ma225/2014Tarefa4-GrupoBtxt.pdf>. Acesso em13 set. 2018.

MORAIS, Rosilda Santos; ONUCHIC, Lourdes de la Rosa. A aprendizagem de polinômios através da resolução de problemas por meio de um ensino contextualizado. **XIII Conferência Interamericana de Educação Matemática**, 2011. Disponível em: <http://www.lematec.net.br/CDS/XIIICIAEM/artigos/1812.pdf>. Acesso em: 13 set. 2018.

SANTOS, José Plínio de Oliveira. **Introdução à teoria dos números**. Rio de Janeiro: IMPA, 2015.

SOUSA, Márcio Monte Alegre. **Divisibilidade em domínios de integridade**. 2013. 27 f. Dissertação (Mestrado Profissional em Matemática) – Universidade Federal de Sergipe, 2013. Disponível em: <https://ri.ufs.br/bitstream/riufs/6474/1/MARCIO_MONTE_ALEGRE_SOUSA.pdf>. Acesso em: 14 set. 2018.

VIEIRA, Ana Cristina. **Fundamentos de álgebra I**. Belo Horizonte: Editora UFMG, 2011.

ISBN 978-85-522-1119-8