HYGINO H. DOMINGUES
Professor da Universidade Estadual Paulista (UNESP)

GELSON IEZZI
Professor da Pontifícia Universidade Católica (SP)

Álgebra Moderna

2ª edição

Capa

Roberto Franklin Rondino
Sylvio Ulhoa Cintra Filho

Composição, desenhos e artes

Atual Editora Ltda.

Fotolitos

H.O.P. Fotolitos Ltda.

CIP-Brasil. Catalogação-na-Publicação
Câmara Brasileira do Livro, SP

D718a 2.ed.

Domingues, Higino Hugueros, 1934-
Álgebra moderna / Hygino H. Domingues, Gelson Iezzi. -- 2. ed. -- São Paulo : Atual, 1982.

Bibliografia.

1. Álgebra I. Iezzi, Gelson, 1939- II. Título.

82-1417

17. CDD-512.89
18. -512

Índices para catálogo sistemático:
1. Álgebra moderna 512.89 (17.) 512 (18.)

PREFÁCIO

O presente texto originou-se no curso básico de Álgebra (três semestres) que os autores tiveram a oportunidade de ministrar na Pontifícia Universidade Católica de São Paulo a partir de 1973. Conseqüentemente, fica patenteado desde logo seu objetivo precipuamente didático. O livro tem um enfoque clássico, praticamente não exige pré-requisitos (os capítulos 0 e I suprem esta parte) e atem-se aos assuntos mais básicos e elementares da Álgebra, com exceção, talvez, do capítulo VI, sobre Anéis Fatoriais, de caráter um pouco mais específico que os demais.

No que se refere à aprendizagem de Álgebra, especialmente nas licenciaturas em Matemática, duas perguntas caracterizam de um modo geral as dificuldades dos estudantes: (a) "Para que serve a Álgebra Moderna?" – tão grande é, muitas vezes, a distância entre os conceitos que estão sendo estudados e as suas possíveis aplicações; (b) "Como se faz para estudar Álgebra, para resolver exercícios de Álgebra?" – indagação que é suscitada de um lado pelo grau de abstração que se faz necessário e, de outro, por não haver em geral nos textos sobre a metéria uma gradação adequada das dificuldades, seja nos exemplos apresentados, seja nos exercícios propostos.

Não foi nosso objetivo apresentar aqui uma resposta à primeira dessas perguntas. Um livro de Álgebra Aplicada necessitaria muito mais material: a ponte entre a teoria e uma aplicação prática é, muitas vezes, mais difícil e laboriosa que a própria teoria (além de se constituir, também, em mais teoria). Cremos que o professor, em suas aulas, em função do próprio currículo de seus alunos, poderia (e deveria) lançar essas "pontes teoria-aplicação", com vistas a motivar ou a justificar, em termos de algo mais "concreto", aquilo que irá ser focalizado em seu curso. Sem querer desprezar a importância que o enfoque dessas possíveis aplicações possa ter em termos de motivação no ensino de Álgebra (muito ao contrário), entendemos que uma boa resposta à segunda das perguntas acima pode ser grandemente decisiva nesse sentido.

Neste particular houve uma tentativa dos autores para melhorar um pouco as coisas: a linguagem do texto é simples, direta, quase sempre auto-suficiente; a simbologia é moderada; no texto da teoria são intercalados exemplos e exercícios resolvidos de fácil entendimento; há uma boa quantidade de exercícios propostos, colocados mais ou menos em ordem crescente de dificuldade (muitos, inclusive, de nível equivalente), com vários resolvidos e respostas para diversos outros.

O capítulo 0, sobre Números Inteiros, não é apenas um pré-requisito para os demais: é também uma oportunidade de apresentar uma introdução suscinta ao assunto, tão importante dentro da Matemática, mas hoje em dia muito esquecido nos currículos de graduação. O capítulo I, sobre "Relações", é bastante longo e esmiuçado pois, além de ser também um pré-requisito para os seguintes, é assunto que em grande parte figura nos programas de Matemática de 1.º e 2.º graus, daí resultando também a extensão com que é apresentado. Os capítulos II e III contêm as noções básicas sobre Grupos, Anéis e Corpos. O capítulo IV, sobre Polinômios, também é bastante detalhado em face da sua importância: entre outras coisas procuramos destacar a diferença entre "polinômio" e "função polinominal" e as coincidências estruturais entre o anel dos inteiros e um anel de polinômios sobre um corpo. As conexões do assunto com a Matemática do 2.º grau também contribuiram para que nele nos detivéssemos um pouco mais. No capítulo V estudam-se as ligações entre estruturas de ordem e algébricas, mas somente a nível de anéis, o que nos parece suficiente tendo em vista a proposta do livro. Finalmente o capítulo VI constitui uma generalização da teoria dos números inteiros e da dos polinômios sobre um corpo, vistas anteriormente, com ligeira incursão a assuntos necessários em graus mais adiantados, por exemplo na Teoria de Galois.

Quanto à redação inicial do livro, coube ao Prof. Hygino H. Domingues escrever a parte de teoria, sendo que o capítulo I foi elaborado juntamente com o Prof. Gelson Iezzi. Quanto aos exercícios (escolha, colocação e resolução) a divisão inicial de trabalho foi a seguinte: Prof. Hygino H. Domingues — capítulos 0 e V; Prof. Gelson Iezzi — demais capítulos. Nesta segunda edição, além das correções feitas, registremos o acréscimo de novos exercícios resolvidos e de respostas a mais alguns exercícios propostos.

Deixamos aqui nossos agradecimentos às equipes de Álgebra da PUC-SP e do IBILCE (Rio Preto) pelas sugestões e observações feitas, de muita valia para esta edição. Ao Prof. Roberto C. F. Costa, da USP, pelo que nos ajudou em termos de leitura de originais para a primeira edição. A todos, enfim, que nos apresentaram sugestões construtivas.

S. Paulo, 1982

Os autores

ÍNDICE

Capítulo 0

NÚMEROS INTEIROS

1. Não faremos aqui uma construção lógico-formal do conjunto dos números inteiros. Nem iremos desenvolver um trabalho sistemático ou profundo sobre o assunto. Admitiremos, de partida, vários pressupostos elementares, visando a obter alguns resultados que serão necessários nos capítulos posteriores, os quais, muitas vezes, não são do conhecimento dos alunos que iniciam um curso de Álgebra.

2. Indicaremos por $\mathbb{Z}$ o conjunto dos números inteiros. Portanto $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$. Admitiremos que já sejam do conhecimento do leitor as propriedades básicas da *adição* e da *multiplicação* em $\mathbb{Z}$ das quais destacaremos as seguintes:

Adição

a) $a + (b + c) = (a + b) + c, \quad \forall\ a, b, c \in \mathbb{Z}$ (associativa)
b) $a + b = b + a, \quad \forall\ a, b \in \mathbb{Z}$ (comutativa)
c) $a + 0 = a, \quad \forall\ a \in \mathbb{Z}$ (0 é o *elemento neutro* da adição)
d) $a + (-a) = 0, \quad \forall\ a \in \mathbb{Z}$ ($-a$ é o *simétrico aditivo* de a)

Multiplicação

a) $a(bc) = (ab)c, \quad \forall\ a, b, c \in \mathbb{Z}$ (associativa)
b) $ab = ba, \quad \forall\ a, b \in \mathbb{Z}$ (comutativa)
c) $a \cdot 1 = a, \quad \forall\ a \in \mathbb{Z}$ (1 é o *elemento neutro* da multiplicação)
d) $ab = 0 \Rightarrow a = 0$ ou $b = 0$ (lei do anulamento do produto)
e) $ab = 1 \Rightarrow a = \pm 1$ e $b = \pm 1$
f) $a(b + c) = ab + ac, \quad \forall\ a, b, c \in \mathbb{Z}$ (a multiplicação é distributiva em relação à adição)

Admitiremos também já conhecida a relação "menor ou igual" em $\mathbb{Z}$, traduzida pelo símbolo "$\leqslant$" e cujas propriedades fundamentais são as seguintes:

a) $a \leqslant a, \quad \forall\, a \in \mathbb{Z}$ (reflexiva)
b) $a \leqslant b \ e \ b \leqslant a \Rightarrow a = b$ (anti-simétrica)
c) $a \leqslant b \ e \ b \leqslant c \Rightarrow a \leqslant c$ (transitiva)
d) Dados a e b em $\mathbb{Z}$, então ou $a \leqslant b$ ou $b \leqslant a$ (totalidade)
e) $a \leqslant b \Rightarrow a + c \leqslant b + c, \quad \forall\, c \in \mathbb{Z}$ (compatibilidade com a adição)
f) $0 \leqslant a \ e \ 0 \leqslant b \Rightarrow 0 \leqslant ab$ (compatibilidade com a multiplicação).

Nota: Um *número inteiro positivo* é um número do subconjunto $\mathbb{Z}_+ = \{0, +1, +2, \ldots\}$ subconjunto esse que pode ser identificado com o conjunto $\mathbb{N} = \{0, 1, 2, \ldots\}$ dos números naturais. Um elemento a de $\mathbb{Z}_+$ se caracteriza pelo fato de que $0 \leqslant a$. Os elementos de $\mathbb{Z}_+^* = \{+1, +2, +3, \ldots\}$ são os *inteiros estritamente positivos*. Dado $a \in \mathbb{Z}$, se $-a \in \mathbb{Z}_+$, dizemos que a é *negativo* e se $-a \in \mathbb{Z}_+^*$ que a é *estritamente negativo*.

g) *Regras de Sinais*

Com o significado óbvio do símbolo "$<$" valem as seguintes implicações:

(i) $0 < a \ e \ 0 < b \Rightarrow 0 < ab$
(ii) $0 < a \ e \ b < 0 \Rightarrow ab < 0$
(iii) $a < 0 \ e \ b < 0 \Rightarrow 0 < ab$

h) *Princípio do menor número inteiro*

Seja L um subconjunto não vazio de $\mathbb{Z}$. Dizemos que L é *limitado inferiormente* se existe um elemento $a \in \mathbb{Z}$ de maneira que $a \leqslant x, \quad \forall\, x \in L$.

O *princípio do menor número inteiro* nos garante o seguinte:

"Se L é um subconjunto não vazio de $\mathbb{Z}$ e L é limitado inferiormente, então existe $\ell_0 \in L$ de maneira que $\ell_0 \leqslant x, \quad \forall\, x \in L$."

É fácil provar que esse elemento ℓ_0 é único. Damos o nome de *mínimo* de L ao elemento ℓ_0 assim definido.

Exemplo

O conjunto $L = \{-2, 0, 2, 4, \ldots\}$ é limitado inferiormente. Os limites inferiores de L são $-2, -3, -4, \ldots$ O mínimo de L é -2.

Um subconjunto $S \subset \mathbb{Z}$ não limitado inferiormente não possui, é claro, mínimo. Por exemplo $S = \{\ldots, -6, -4, -2, 0\}$ não é limitado inferiormente. Não existe portanto o mínimo de S.

3. Indução

Primeiro princípio de indução

Apesar da designação clássica trata-se de uma proposição relativamente fácil de provar a partir dos pressupostos com que já contamos. Seu enunciado é o seguinte:

"Dado $a \in \mathbb{Z}$, suponhamos que a cada inteiro $n \geqslant a$ esteja associada uma afirmação $P(n)$. Então, $P(n)$ será verdadeira para todo $n \geqslant a$ desde que seja possível provar o seguinte:

(i) $P(a)$ é verdadeira;
(ii) Se $P(r)$ é verdadeira para $r \geqslant a$, então $P(r+1)$ também é verdadeira."

Como o artifício e o raciocínio usados para provar esse "princípio" são os mesmos usados para demonstrar o "segundo princípio de indução", que será visto a seguir, omitiremos a demonstração deste primeiro para fazer apenas a do segundo.

Exemplo: Provar que $1 + n \leqslant 2^n, \quad \forall\, n \geqslant 0$.

$n = 0$: $1 + 0 \leqslant 2^0$ é óbviamente verdadeira.

Suponhamos $1 + r \leqslant 2^r$, com $0 \leqslant r$. Então $2 + r \leqslant 2 + 2r = 2(1 + r) \leqslant 2 \cdot 2^r = 2^{r+1}$

Daí: $1 + (1 + r) \leqslant 2^{r+1}$.

Segundo princípio de indução

"Dado $a \in \mathbb{Z}$, suponhamos que a cada inteiro $n \geqslant a$ esteja associada uma afirmação $P(n)$. Então $P(n)$ será verdadeira para todo $n \geqslant a$, desde que seja possível provar o seguinte:

(i) $P(a)$ é verdadeira;
(ii) Dado $r > a$, se $P(k)$ é verdadeira para todo k tal que $a \leqslant k < r$, então $P(r)$ é verdadeira."

Demonstração: Seja $L = \{x \in \mathbb{Z} \mid a \leqslant x \ e \ P(x) \text{ é falsa}\}$. Mostremos que $L = \phi$. Se $L \neq \phi$, como L é limitado inferiormente, então existe o mínimo ℓ_0 de L. Devido à (i) $\ell_0 \neq a$. Sendo ℓ_0 o mínimo de L, então $P(x)$ é verdadeira para todo elemento x de $\mathbb{Z}$ tal que $a \leqslant x < \ell_0$.

Então podemos concluir, com base em (ii), que $P(\ell_0)$ é verdadeira. Absurdo. Esta contradição prova que a afirmação do princípio é verdadeira. ■

4. Múltiplos e divisores

Seja a um número inteiro. Os *múltiplos* de a são os números

$$0, \pm a, \pm 2a, \ldots$$

ou seja, os números ka, onde k é um elemento qualquer de $\mathbb{Z}$. Evidentemente se ka e ha são múltiplos de a, então sua soma e seu produto

$$ha + ka = (h + k)a \quad e \quad (ha)(ka) = (hak)a$$

também são múltiplos de a.

Quando se tem $c = ab$, a, b, $c \in \mathbb{Z}$, dizemos que a é um *divisor* de c ou que a *divide* c e que c é *divisível por* a. Notação: $a \mid c$. Para a relação assim definida vale o seguinte:

(a) $a \mid a$, $\forall\, a \in \mathbb{Z}$, pois $a = a \cdot 1$.

(b) Se $a \mid b$ e $b \mid a$ e, ainda, $a, b \in \mathbb{Z}_+$, então $a = b$.

Com efeito, $b = ac_1$ e $a = bc_2$. Se $a = 0$ ($b = 0$), então $b = 0$ ($a = 0$). Caso contrário teremos $c_1 > 0$ e $c_2 > 0$. Como $a = a(c_1 c_2)$, então $c_1 c_2 = 1$. Donde $c_1 = c_2 = 1$ e $a = b$.

(c) Se $a \mid b$ e $b \mid c$, então $a \mid c$.

De fato, por hipótese temos $b = ad_1$ e $c = bd_2$. Daí $c = a(d_1 d_2)$.

(d) Se $a \mid b$ e $a \mid c$, então $a \mid (bx + cy)$, $\forall\, x, y \in \mathbb{Z}$.

Provemos. Por hipótese $b = ad_1$ e $c = ad_2$. Logo $bx = a(xd_1)$ e $cy = a(yd_2)$. Portanto $bx + cy = a(xd_1 + yd_2)$ o que vem mostrar que a divide $bx + cy$.

5. Algorítmo da divisão

Seja b um número inteiro estritamente positivo. Dado $a \in \mathbb{Z}$, então ou a é um múltiplo de b ou está situado entre dois múltiplos consecutivos qb e $(q + 1)b$ de b: $qb < a < (q + 1)b$. Neste caso tem-se

$$0 < a - qb < b$$

o que se obtém somando $-(qb)$ às desigualdades anteriores. Fazendo $r = a - qb$ obtemos

$$a = bq + r, \text{ onde } 0 < r < b.$$

Sintetizando os dois casos podemos dizer que

"Dados a, $b \in \mathbb{Z}$, com b estritamente positivo, existem q, $r \in \mathbb{Z}$, de maneira que $a = bq + r$ e $0 \leqslant r < b$."

Obviamente $r = 0$ quando a é múltiplo de b.

Suponhamos agora $a = bq + r = bq_1 + r_1$, onde $0 \leqslant r, r_1 < b$. Admitamos que se pudesse ter $r \neq r_1$, por exemplo $r > r_1$. Como

$$b(q_1 - q) = r - r_1$$

teríamos então $q_1 > q$. Assim

$$r = r_1 + b(q_1 - q)$$

Ora, sendo $r_1 \geqslant 0$ e $q_1 - q \geqslant 1$, conclui-se desta última igualdade que $r \geqslant b$ o que é absurdo. Então $r = r_1$ e, consequentemente, $q_1 = q$. ■

Os elementos q e r acima, cuja unicidade acabamos de provar, chamam-se, respectivamente, *quociente* e *resto* na divisão euclidiana de a por b.

O resultado que acabamos de obter recebe a designação de *algorítmo da divisão* ou *algorítmo de Euclides* em $\mathbb{Z}$.

Exemplos

(i) $a = 60$ e $b = 7$. Neste caso $60 = 7 \cdot 8 + 4$, onde $q = 8$ e $r = 4$.
(ii) $a = -60$ e $b = 7$. Aqui, $-60 = 7 \cdot (-9) + 3$, $q = -9$ e $r = 3$.

6. Máximo divisor comum

Definição 1: Dados a, $b \in \mathbb{Z}$, dizemos que $d \in \mathbb{Z}$ é *máximo divisor comum* entre a e b se (i) $d \geqslant 0$; (ii) $d \mid a$ e $d \mid b$ e (iii) se d' é um número inteiro tal que $d' \mid a$ e $d' \mid b$, então $d' \mid d$.

Observações

a) Se d e d_1 são máximos divisores comuns entre a e b, então $d = d_1$. De fato, como $d \mid d_1$ e $d_1 \mid d$ e, ainda, são ambos positivos, concluímos que $d = d_1$;
b) Se $a = b = 0$, então $d = 0$, como é óbvio;
c) Se $a = 0$ e $b \neq 0$, então $d = |b|$;
d) Se d é máximo divisor comum entre a e b, então d também é máximo divisor comum entre a e $-b$, $-a$ e b e, ainda, entre $-a$ e $-b$, o que não oferece dificuldade nenhuma provar.

Notação: Indicaremos por mdc (a, b) o máximo divisor comum entre a e b que já sabemos ser único, quando existe. A proposição a seguir nos garante sua existência em todos os casos.

Proposição 1: Quaisquer que sejam a, $b \in \mathbb{Z}$, existe $d \in \mathbb{Z}$ que é o máximo divisor comum de a e b.

Demonstração: Levando em conta as observações acima podemos nos limitar ao caso em que $a > 0$ e $b > 0$.

Seja $L = \{ax + by \mid x, y \in \mathbb{Z}\}$. Evidentemente existem elementos estritamente positivos em L (faça-se, por exemplo, $x = y = 1$). Seja d o menor desses elementos. Mostremos que d é o máximo divisor comum entre a e b.

(i) d é óbviamente maior que zero;

(ii) Como $d \in L$, então existem $x_0, y_0 \in \mathbb{Z}$ de maneira que $d = ax_0 + by_0$. Aplicando o algorítmo da divisão aos elementos a e d:

$a = dq + r \quad (0 \leqslant r < d)$.

Das duas últimas igualdades tiramos

$$a = (ax_0 + by_0)q + r$$

ou, ainda

$$r = a(1 - qx_0) + b(-y_0)q$$

o que vem mostrar que $r \in L$. Sendo r positivo e levando em conta a escolha do elemento d a conclusão é que $r = 0$. Daí ficamos com $a = dq$ o que mostra que $d \mid a$. Analogamente se prova que $d \mid b$;

(iii) Se $d' \mid a$ e $d' \mid b$, como $d = ax_0 + by_0$, então é claro que $d' \mid d$. ■

Nota: Se $d = mdc(a, b)$, então se verificou, na demonstração acima, que $d = ax_0 + by_0$, onde $x_0, y_0 \in \mathbb{Z}$. Os elementos x_0 e y_0 que satisfazem tal identidade não são únicos. Uma tal identidade recebe o nome de *identidade de Bezout* em $\mathbb{Z}$ para os elementos a e b.

7. Números primos

Definição 2: Um número $p \in \mathbb{Z}$ é chamado *número primo* se (i) $p \neq 0$; (ii) $p \neq \pm 1$ e (iii) os únicos divisores de p são $1, -1, p$ e $-p$.

Observação: Os divisores $a, -a, 1$ e -1 de $a \in \mathbb{Z}$ são chamados *divisores triviais* de a. Dizer que a *não é primo* significa, quando $a \neq 0$ e $a \neq \pm 1$, que existem outros divisores de a além dos triviais. Um número $a \in \mathbb{Z}$ tal que $a \neq 0$, $a \neq \pm 1$, e não primo será chamado de número inteiro *composto*. Por exemplo, o número 6 é composto pois além dos divisores $1, -1, 6$ e -6 triviais, admite também os divisores $2, -2, 3$ e -3.

Proposição 2: Se p é primo e $p \mid ab$, então $p \mid a$ ou $p \mid b$. (Por indução, se $p \mid a_1 a_2 \ldots a_n$, então p divide um dos a_i.) (Lema de Euclides)

Demonstração: Suponhamos que p não seja divisor de a. Então os divisores comuns de p e a são apenas 1 e -1. Daí $mdc(a, p) = 1$. Logo existem $x_0, y_0 \in \mathbb{Z}$ de maneira que

$$1 = ax_0 + py_0.$$

Portanto

$$b = (ab)x_0 + p(by_0).$$

Como $p \mid (ab)$ e $p \mid p$, então $p \mid b$. ■

Proposição 3: Seja a um número inteiro não nulo e diferente de ± 1. Então o mínimo do conjunto $S = \{x \in \mathbb{Z} \mid x > 1 \text{ e } x \mid a\}$ é um número primo.

Demonstração: Como a e $-a$ são divisores de a é óbvio que $S \neq \phi$.

Seja p o menor dos elementos de S. Se p não fosse primo, então existiria um divisor não trivial q de p. Como $(-q)$ também será um divisor de p, pode-se dizer que existe um divisor q_1 de $p (q_1 = q$ ou $q_1 = -q)$ tal que $1 < q_1 < p$. Mas de $p \mid a$ e $q_1 \mid p$ decorre que $q_1 \mid a$ que significa que $q_1 \in S$. Absurdo pois p é o mínimo de S.

Teorema 1 (Teorema fundamental da aritmética): Dado um número inteiro $a > 1$, existem r números inteiros primos estritamente positivos $p_1, \ldots, p_r$ de maneira que $a = p_1 p_2 \ldots p_r$ $(r \geqslant 1)$. Além disso, se tivermos também $a = q_1 q_2 \ldots q_s$, onde os q_j são primos estritamente positivos, então $r = s$ e cada p_i é igual a um dos q_j.

Demonstração: (a) Usaremos o segundo princípio de indução. Se $a = 2$, então a afirmação do enunciado é válida pois o número 2 é primo.

Suponhamos o teorema válido para todo $b \in \mathbb{Z}$ tal que $2 \leqslant b < a$. A proposição 3 nos garante que existe um número primo $p_1 > 0$ que divide a: $a = p_1 a_1$. Se $a_1 = 1$ ou a_1 é primo, a conclusão é imediata. Caso contrário, como $2 \leqslant a_1 < a$, a hipótese de indução nos garante que $a_1 = p_2 \ldots p_r$ $(r - 1 \geqslant 1)$, onde os p_i são estritamente positivos e primos. Logo

$$a = p_1 p_2 \ldots p_r.$$

(ii) $p_1 \ldots p_r = q_1 \ldots q_s \Longrightarrow p_1 \mid q_1 q_2 \ldots q_s \Longrightarrow p_1 \mid q_j$ $(1 \leqslant j \leqslant s)$, devido à proposição 2.

Suponhamos $j = 1$. Então $p_1 \mid q_1$ e daí $p_1 = q_1$ uma vez que q_1 é primo e $p_1 > 1$. Cancelando p_1 e q_1 na igualdade inicial e prosseguindo com o raciocínio desenvolvido até aqui, chega-se à unicidade da decomposição. ■

Corolário: Seja a um número inteiro não nulo e diferente de ± 1. Então existem (e são únicos) os números primos estritamente positivos $p_1, \ldots, p_r$ $(r \geqslant 1)$, de maneira que $a = \pm p_1 \ldots p_r$.

Demonstração: evidente. ■

8. Congruências

Definição 3: Seja $m > 1$ um número inteiro. Dados $a, b \in \mathbb{Z}$, dizemos que *a é côngruo a b*, módulo m, se, e somente se, $m \mid (a - b)$.

Notação: $a \equiv b \pmod{m}$.

Exemplos

(a) $21 \equiv 1 \pmod 5$ pois $21 - 1 = 20$ é divisível por 5.

(b) $100 \equiv 1 \pmod 9$ pois $100 - 1 = 99$ é múltiplo de 9.

Propriedades

(a) $a \equiv a \pmod m$, $\forall\, a \in \mathbb{Z}$, pois $a - a = 0$ é divisível por m.

(b) $a \equiv b \pmod m \Longrightarrow b \equiv a \pmod m$.

De fato, se $m \mid (a - b)$, então $m \mid (b - a)$, pois $b - a = -(a - b)$.

(c) $a \equiv b \pmod m$ e $b \equiv c \pmod m \Longrightarrow a \equiv c \pmod m$.

Provemos. Como $m \mid (a - b)$ e $m \mid (b - c)$, então $m \mid [(a - b) + (b - c)]$, ou seja, $m \mid (a - c)$. Isto equivale à tese.

(d) $a \equiv b \pmod m$ e $c \equiv d \pmod m \Rightarrow a + c \equiv b + d \pmod m$.

Fica como exercício a verificação desta propriedade.

(e) $a \equiv b \pmod m \Longrightarrow ac \equiv bc \pmod m$, $\forall\, c \in \mathbb{Z}$.

Exercício.

(f) $a \equiv b \pmod m \Longrightarrow a^r \equiv b^r \pmod m$, $\forall\, r \geqslant 1$.

Para $r = 1$ a implicação é evidente.

Suponhamos $a^r \equiv b^r \pmod m$. Então $a^{r+1} \equiv ab^r \pmod m$. Por outro lado, de $a \equiv b \pmod m$, segue que $ab^r \equiv b^{r+1} \pmod m$. Juntando as duas conclusões tiramos $a^{r+1} \equiv b^{r+1} \pmod m$.

Exemplo: Critério de divisibilidade por 3.

A relação definida acima no conjunto $\mathbb{Z}$, que denominamos *congruência*, pode ser usada para explicar o critério de divisibilidade por 3, entre outros, da maneira como veremos a seguir.

Um número natural $a \geqslant 1$ sempre admite a decomposição

$$a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots + a_r \cdot 10^r$$

quando se usa a base 10 para o sistema de numeração. Nessa representação, que é única, a_0 é o algarismo das unidades, a_1 o das dezenas, e assim por diante. Então:

$a_0 \equiv a_0 \pmod 3$

$10a_1 \equiv a_1 \pmod 3$, pois $10 \equiv 1 \pmod 3$

$10^2 a_2 \equiv a_2 \pmod 3$, pois $10^2 \equiv 1 \pmod 3$

. . . . . .

Somando as congruências acima de acordo com a propriedade (d) achamos

$$a \equiv a_0 + a_1 + \ldots + a_r \pmod 3.$$

Disto se tira a seguinte conclusão: se $a_1 + \ldots + a_r$ for divisível por 3, isto é, côngruo a zero módulo 3, o número a também será divisível por 3, e vice-versa.

EXERCÍCIOS

1. Prove por indução:

a) $1 + 2 + 3 + \ldots + n = \dfrac{n(n+1)}{2}$, $\forall\, n \in \mathbb{N}$, $n \geqslant 1$.

b) $1^2 + 2^2 + 3^2 + \ldots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$, $\forall\, n \in \mathbb{N}$, $n \geqslant 1$.

c) $0 < a \Longrightarrow 0 < a^n$, $\forall\, n \in \mathbb{N}$.

Observação: define-se a^r assim: $a^0 = 1$ e $a^r = a^{r-1} \cdot a$, $\forall\, r > 0$.

d) $a^m \cdot a^n = a^{m+n}$, $\forall\, m, n \in \mathbb{N}$. (Indução sobre n, fixando m)

e) $(a^m)^n = a^{mn}$, $\forall\, m, n \in \mathbb{N}$.

f) $a < 0 \Longrightarrow 0 < a^{2n}$ e $a^{2n+1} < 0$, $\forall\, n \in \mathbb{N}$.

g) $2^{2n-1} \cdot 3^{n+2} + 1$ é divisível por 11, $\forall\, n \in \mathbb{N}$, $n \geqslant 1$.

h) $3^{2n+1} + 2^{n+2}$ é divisível por 7, $\forall\, n \in \mathbb{N}$.

i) $2^{2n} + 15n - 1$ é divisível por 9, $\forall\, n \in \mathbb{N}$, $n \geqslant 1$.

j) $3^{4n+2} + 2 \cdot 4^{3n+1}$ é múltiplo de 17, $\forall\, n \in \mathbb{N}$.

2. Sejam $a, b, c \in \mathbb{N}^*$ números sem divisores comuns tais que $a^2 + b^2 = c^2$.

a) Mostre que ou a ou b é par;

b) Mostre que ou a ou b é múltiplo de 3.

3. Mostre que o quadrado de um número ímpar é da forma $8q + 1$, $q \in \mathbb{Z}$.

4. Seja $a \in \mathbb{Z}$ um número não divisível por 5. Mostre que $a^4 = 5q + 1$, $q \in \mathbb{Z}$.

Sugestão: examinar as quatro possibilidades para a, isto é, $a \equiv 1$ ou $a \equiv 2$ ou $a \equiv 3$ ou $a \equiv 4 \pmod 5$.

5. Sejam $a, b \in \mathbb{Z}$ de modo que $\text{mdc}(a, b) = 1$. Se $a \mid c$ e $b \mid c$, mostre que $ab \mid c$.

6. Use o resultado do exercício anterior para provar que $6 \mid n(2n + 7)(7n + 1)$, $\forall\, n \in \mathbb{Z}$.

Solução:

Basta provar que $2 \mid n(2n + 7)(7n + 1)$ e que $3 \mid n(2n + 7)(7n + 1)$ visto que $\text{mdc}(2, 3) = 1$. Se n é par, então $2 \mid n$ e logo $2 \mid n(2n + 7)(7n + 1)$. Se $n = 2t + 1$ (ímpar), então $7n + 1 = 14t + 8 = 2(7t + 4)$ e portanto $2 \mid n(2n + 7)(7n + 1)$. Para provar que $3 \mid n(2n + 7)(7n + 1)$ basta considerar os casos $n = 3t$, $n = 3t + 1$ e $n = 3t + 2$ e proceder analogamente.

7. Mostre que, para todo inteiro n, o máximo divisor comum entre $2n + 1$ e $\dfrac{n(n+1)}{2}$ é 1.

8. Prove que $\text{mdc}(a, b) = \text{mdc}(a + bc,\ a + b(c - 1))$, $\forall\, a, b, c \in \mathbb{Z}$.

Sugestão: mostre que todo divisor de a e b é divisor de $a + bc$ e $a + b(c - 1)$ e vice-versa.

9. Mostre que $a^3 - a$ é múltiplo de 3, $\forall\, a \in \mathbb{Z}$.

10. Mostre que $a^3 - b^3$ é múltiplo de 3 se, e somente se, $a - b$ é múltiplo de 3.

11. Mostre que $6 \mid n(n+1)(2n+1)$, $\forall\, n \in \mathbb{Z}$.

12. Mostre que $30 \mid n(n^2-49)(n^2+49)$, $\forall\, n \in \mathbb{Z}$.

13. Ache o resto da divisão de $a = 531 \cdot 31^2 \cdot 2$ por 7.

14. Ache o algarismo das unidades dos números $9^{(9^9)}$ e $7^{(7^7)}$.

Solução:

O algarismo das unidades de $7^{(7^7)}$ é o resto na divisão euclidiana deste número por 10. Temos: $7 \equiv 7 \pmod{10}$, $7^2 \equiv 9 \pmod{10}$, $7^3 \equiv 3 \pmod{10}$, $7^4 \equiv 1 \pmod{10}$ e, daqui em diante, os resultados se repetem ciclicamente módulo 4. Logo basta situar o expoente 7^7 quanto a este aspecto. Ora: $7 \equiv 3 \pmod 4$, $7^2 \equiv 1 \pmod 4$ e portanto $7^7 \equiv 3 \pmod 4$. Assim o expoente 7^7 está na mesma classe do expoente 3, módulo 4, e consequentemente $7^{(7^7)} \equiv 7^3 \equiv 3 \pmod{10}$. Donde o algarismo das unidades procurado é 3.

15. Ache os dois últimos algarismos de $7^{(7^{1000})}$.

16. Enuncie e justifique critérios de divisibilidade por 9, 5, 11 e 6.

17. Mostre que o conjunto dos números primos positivos é infinito.

Sugestão: suponha que os números primos positivos formem um conjunto finito. Sejam $p_1, p_2, \ldots, p_r$ os primos positivos. Mostre que $p_1 \cdot p_2 \cdot p_3 \ldots p_r + 1$ é primo positivo e diferente dos p_i anteriores, o que é absurdo.

18. Sejam $a, b, c \in \mathbb{Z}$ números tais que $a \mid bc$ e $\text{mdc}(a, b) = 1$. Prove que $a \mid c$.
Sugestão: use a identidade de Bézout.

19. Mostre que se p é primo, então $p \mid \binom{p}{i}$ onde $0 < i < p$.

Solução:

Como $\binom{p}{i} = \dfrac{p(p-1)\ldots(p-i+1)}{i!}$, então $p(p-1)\ldots(p-i+1) = \binom{p}{i} \cdot i!$.

Donde $p \mid \binom{p}{i} i!$ e, como $p \nmid i!$ (se dividisse teria que dividir i ou $i-1$ ou $\ldots$ ou 1 o que não é possível pois $i < p$), então $p \mid \binom{p}{i}$, já que p é primo.

20. Sejam $a, b \in \mathbb{Z}$. Se existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1$, mostre que $\text{mdc}(a, b) = 1$.

Capítulo I

RELAÇÕES APLICAÇÕES OPERAÇÕES

§ 1º — RELAÇÕES BINÁRIAS

1. DEFINIÇÃO

Definição 1: Dados dois conjuntos E e F, não vazios, chama-se *produto cartesiano de E por F* o conjunto formado por todos os "pares ordenados" (x, y) com x em E e y em F. Costuma-se indicar o produto cartesiano de E por F com a notação E x F (lê-se: "E cartesiano F"). Assim, temos:

$$E \times F = \{(x, y) \mid x \in E \text{ e } y \in F\}$$

Definição 2: Chama-se *relação binária de E em F* todo subconjunto R de E x F.

(R é relação de E em F) $\iff$ $R \subset E \times F$

A definição deixa claro que toda relação é um conjunto de pares ordenados. Para indicar que $(a, b) \in R$ usaremos algumas vezes a notação a R b (lê-se: "a erre b" ou "a relaciona-se com b segundo R"). Se $(a, b) \notin R$, escreveremos a $\not R$ b.

Os conjuntos E e F são denominados, respectivamente, *conjunto de partida* e *conjunto de chegada* da relação R.

2. EXEMPLOS

1º) Se $E = \{0, 1, 2\}$ e $F = \{-2, -1, 0, 1, 2\}$, então:

$E \times F = \{(0, -2), (0, -1), (0, 0), (0, 1), (0, 2), (1, -2), (1, -1), (1, 0), (1, 1), (1, 2), (2, -2), (2, -1), (2, 0), (2, 1), (2, 2)\}$

Qualquer subconjunto de ExF é uma relação de E em F; então são exemplos de relações:

$R_1 = \{(0, 0), (1, -1), (1, 1)\}$

$R_2 = \{(0, 1), (1, 2), (2, -2), (0, -1), (1, 0)\}$

$R_3 = \{(2, -2)\}$

ϕ

2º) Se $E = F = \mathbb{Z}$, então ExF é o conjunto formado por todos os pares ordenados de números inteiros. Um exemplo de relação de $\mathbb{Z}$ em $\mathbb{Z}$ é:

$R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x = y\} =$

$= \{\ldots (-n, -n), \ldots, (-1, -1), (0, 0), (1, 1), \ldots, (n, n), \ldots\}$

3º) Se $E = F = \mathbb{R}$, então ExF é o conjunto formado por todos os pares ordenados de números reais. Um exemplo de relação de $\mathbb{R}$ em $\mathbb{R}$ é:

$R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y \geqslant 0\}$

3. DOMÍNIO E IMAGEM

Seja R uma relação de E em F.

Definição 3: Chama-se *domínio de R* o subconjunto de E constituído pelos elementos x para cada um dos quais existe algum y em F tal que xRy. Em símbolos:

$$D(R) = \{x \in E \mid \exists\, y \in F \ni xRy\}$$

Definição 4: Chama-se *imagem de R* o subconjunto de F constituído pelos elementos y para cada um dos quais existe algum x em E tal que xRy. Simbolicamente, temos:

$$Im(R) = \{y \in F \mid \exists\, x \in E : xRy\}$$

Em outros termos, D(R) é o conjunto formado pelos primeiros termos dos pares ordenados que constituem R e Im(R) é formado pelos segundos termos dos pares de R.

Assim, voltando aos exemplos anteriores, temos:

1º) $D(R_1) = \{0, 1\}$ e $Im(R_1) = \{0, -1, 1\}$

$D(R_2) = \{0, 1, 2\}$ e $Im(R_2) = \{-2, -1, 0, 1, 2\}$

$D(R_3) = \{2\}$ e $Im(R_3) = \{-2\}$

2º) $D(R) = \mathbb{Z}$ e $Im(R) = \mathbb{Z}$

3º) $D(R) = \mathbb{R}$ e $Im(R) = \mathbb{R}_+$

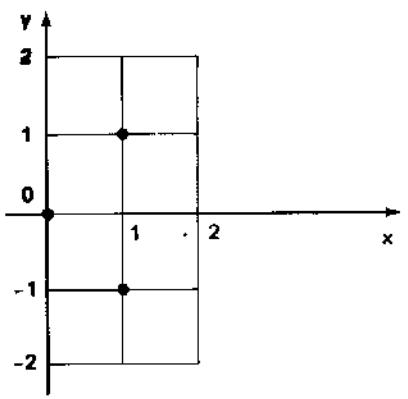
REPRESENTAÇÕES

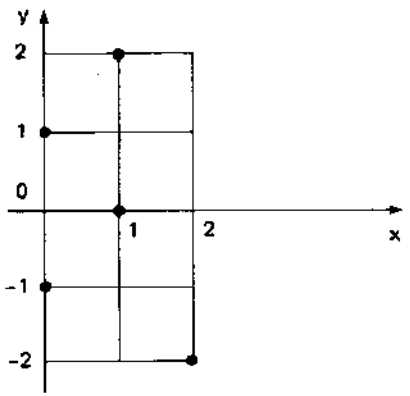
a) gráfico cartesiano

Grande parte das relações de que se trata em Matemática são relações em que E (conjunto de partida) e F (conjunto de chegada) são subconjuntos de $\mathbb{R}$. Nesses casos, o gráfico da relação é o conjunto dos pontos de um plano dotado de um sistema de coordenadas cartesianas ortogonais, cujas abscissas são os primeiros termos e as ordenadas os segundos termos dos pares que constituem a relação.

Exemplos

1º) $R_1 = \{(0, 0), (1, -1), (1, 1)\}$ $\quad R_2 = \{(0, 1), (1, 2), (2, -2), (0, -1), (1, 0)\}$

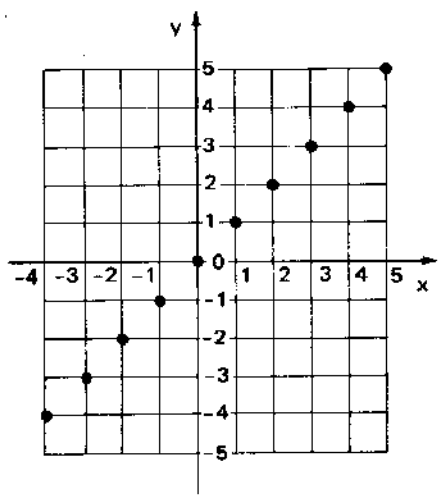




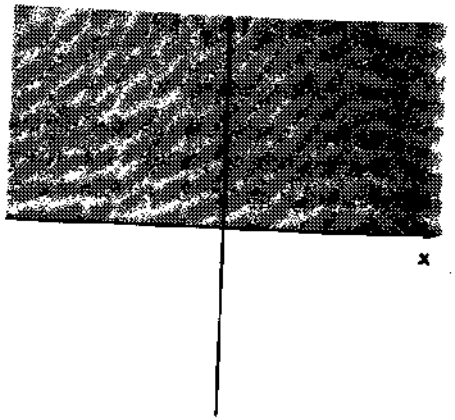
2º) $E = \mathbb{Z}$

$F = \mathbb{Z}$

$R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x = y\}$



3º) $E = \mathbb{R}$
$F = \mathbb{R}$
$R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y \geqslant 0\}$

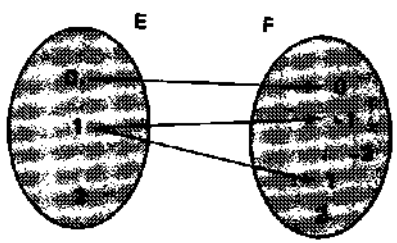


b) *esquema de flechas*

Quando E e F são conjuntos finitos com "poucos" elementos, podemos representar uma relação R de E em F da seguinte forma: representamos E e F por meio de diagramas de Venn e indicamos cada $(x, y) \in R$ por uma flecha com "origem" x e "extremidade" y.

Exemplo

$E = \{0, 1, 2\}$
$F = \{-2, -1, 0, 1, 2\}$
$R = \{(0, 0), (1, -1), (1, 1)\}$



5. INVERSA DE UMA RELAÇÃO

Definição 5: Seja R uma relação de E em F. Chama-se *relação inversa de R*, e indica-se por R^{-1}, a seguinte relação de F em E:

$R^{-1} = \{(y, x) \in F \times E \mid (x, y) \in R\}$

Exemplos

1º) Se $E = \{a_1, a_2, a_3\}$, $F = \{b_1, b_2, b_3, b_4\}$ e $R = \{(a_1, b_1), (a_1, b_2), (a_2, b_3), (a_3, b_4)\}$, então:
$R^{-1} = \{(b_1, a_1), (b_2, a_1), (b_3, a_2), (b_4, a_3)\}$

2º) Se $E = F = \mathbb{R}$ e $R = \{(x, y) \in \mathbb{R}^2 \mid y = 2x\}$, então
$R^{-1} = \{(y, x) \in \mathbb{R}^2 \mid y = 2x\} = \{(x, y) \in \mathbb{R}^2 \mid x = 2y\}$

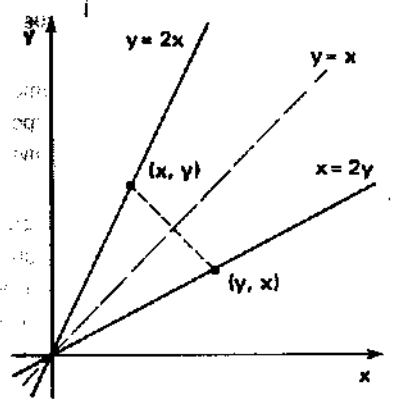
3º) Se $E = F = \mathbb{R}$ e $R = \{(x, y) \in \mathbb{R}^2 \mid x^2 + (y-2)^2 \leqslant 1\}$, então:
$R^{-1} = \{(y, x) \in \mathbb{R}^2 \mid x^2 + (y-2)^2 \leqslant 1\} = \{(x, y) \in \mathbb{R}^2 \mid y^2 + (x-2)^2 \leqslant 1\}$

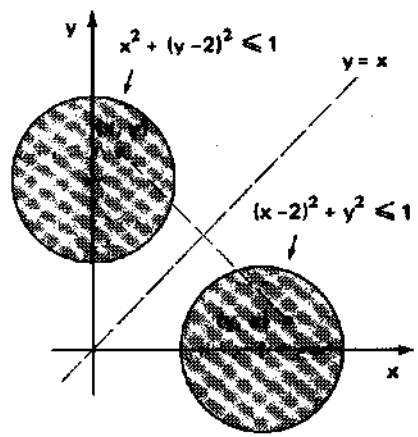
Representação de R^{-1}

a) Se a relação R admite um gráfico cartesiano, então o mesmo ocorre com R^{-1}. Notando que:

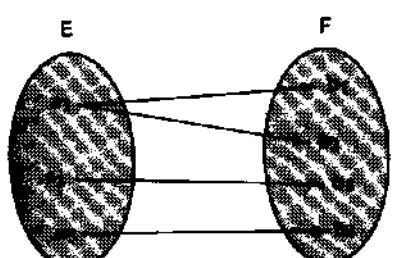
$$(x, y) \in R \iff (y, x) \in R^{-1},$$

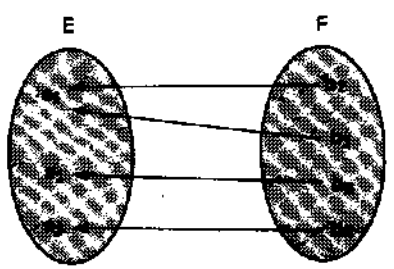
fica evidente que o gráfico cartesiano de R^{-1} é simétrico do gráfico de R, em relação à reta de equação $y = x$. Exemplos:





b) Dado o diagrama de Euler-Venn de uma relação R, obtemos o diagrama de R^{-1} simplesmente invertendo o sentido das flechas. Por exemplo, se $E = \{a_1, a_2, a_3\}$, $F = \{b_1, b_2, b_3, b_4\}$ e $R = \{(a_1, b_1), (a_1, b_2), (a_2, b_3), (a_3, b_4)\}$, temos:





então é, $R^{-1} = \{(b_1, a_1), (b_2, a_1), (b_3, a_2), (b_4, a_3)\}$

Propriedades: são facilmente demonstráveis as propriedades seguintes para R^{-1}:

a) $D(R^{-1}) = Im(R)$

b) $Im(R^{-1}) = D(R)$

c) $(R^{-1})^{-1} = R$

Deixamos a prova como exercício.

6. RELAÇÃO SOBRE UM CONJUNTO

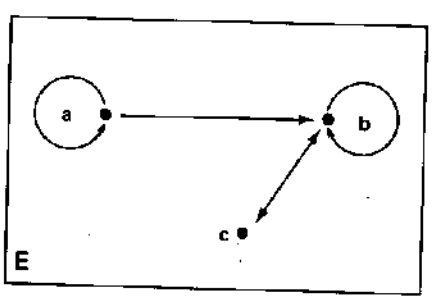
Definição 6: Quando E = F e R é uma relação de E em F, diz-se que *R é uma relação sobre E*, ou ainda, *R é uma relação em E*.

As relações sobre E vão merecer um destaque especial neste livro. Veremos algumas propriedades que podem apresentar e, a seguir, estudaremos dois tipos de relações sobre E que têm características importantes: as relações de equivalência e as relações de ordem.

No estudo das relações sobre um conjunto E, com E finito e tendo "poucos" elementos, é muito útil a representação através do esquema de flechas, que pode ser assim simplificado: representamos o conjunto E com seus elementos e indicamos cada par (a, b) da relação através de uma flecha com "origem" *a* e "extremidade" *b*. Se (a, a) está na relação, usa-se um "laço" envolvendo a, conforme exemplo a seguir.

Exemplo

O esquema ao lado representa a relação
R = {(a, a), (b, b), (a, b), (b, c), (c, b)} sobre E = {a, b, c}.



7. PROPRIEDADES

Daremos a seguir as principais propriedades que uma relação R sobre um conjunto E pode verificar.

a) Reflexiva

Dizemos que R é reflexiva quando está satisfeita a condição:

$(\forall\ x)\ (x \in E \implies x\ R\ x)$

, isto é, R é reflexiva se todo elemento de E se relaciona consigo mesmo.

Se designarmos com Δ_E o conjunto $\Delta_E = \{(x, x) \mid x \in E\}$, então R é reflexiva quando $\Delta_E \subset R$.

Exemplos

1º) A relação R = {(a, a), (b, b), (c, c), (a, c), (b, a)} sobre E = {a, b, c} é reflexiva pois aRa, bRb, e cRc.

2º) A relação R de igualdade sobre o conjunto $\mathbb{R}$ dos números reais: $xRy \iff x = y$ é uma relação reflexiva pois, para todo x real, $x = x$.

3º) A relação R de paralelismo definida sobre o conjunto E das retas do espaço:

$$xRy \iff x \parallel y$$

é reflexiva pois, para toda reta x, $x \parallel x$.

Contra-exemplo

Notemos que uma relação R sobre E *não* é reflexiva quando existir um elemento x em E tal que $x \not R\ x$. Assim, por exemplo, a relação R = {(a, a), (b, b), (a, b), (b, a), (a, c), (c, a), (b, c), (c, b)} sobre E = {a, b, c} não é reflexiva pois $c \not R c$.

b) Simétrica

Dizemos que R é simétrica quando está satisfeita a seguinte condição:

$(\forall\ x, y \in E)\ (x\ R\ y \implies y\ R\ x)$

isto é, R é simétrica quando, estando x relacionado com y, temos também y relacionado com x.

Exemplos

1º) A relação R = {(a, a), (a, b), (b, a), (b, b)} é uma relação simétrica sobre E = {a, b, c}.

2º) A relação R de perpendicularismo definida sobre o conjunto E das retas do espaço:

$$xR\,y \iff x \perp y$$

é simétrica pois, para duas retas x e y quaisquer, $x \perp y \implies y \perp x$.

3º) A relação R sobre $\mathbb{Q}$ (conjunto dos números racionais) definida por: $x\ R\ y \iff x^2 = y^2$ é simétrica pois, para dois racionais x e y quaisquer, $x^2 = y^2 \implies y^2 = x^2$.

Contra-exemplo

Notemos que uma relação R sobre E *não* é simétrica se existirem $x \in E$ e $y \in E$ tais que xRy e $y \not R x$. Assim, por exemplo, a relação R = {(a, a), (b, b), (c, c), (a, b)} sobre E = {a, b, c} não é simétrica pois aRb e $b \not R a$.

c) Transitiva

Dizemos que R é transitiva quando está satisfeita a condição:

$(\forall x, y, z \in E)\ (x R y \text{ e } y R z \implies x R z)$

isto é, se x está relacionado com y e y está relacionado com z, então x está relacionado com z.

Exemplos

1º) A relação $R = \{(a, a), (a, b), (b, c), (a, c)\}$ sobre $E = \{a, b, c\}$ é transitiva.

2º) A relação R de semelhança definida sobre o conjunto E dos triângulos do espaço:

$$x R y \iff x \sim y$$

é transitiva pois, sendo x, y e z triângulos quaisquer, $x \sim y$ e $y \sim z \Rightarrow x \sim z$.

3º) A relação R sobre $\mathbb{N}$ (conjunto dos números naturais) definida por: $xRy \iff x \leqslant y$ é transitiva pois, dados três naturais x, y e z, se $x \leqslant y$ e $y \leqslant z$ então $x \leqslant z$.

Contra-exemplo

Notemos que uma relação R sobre E *não* é transitiva se existirem $x, y, z \in E$ tais que xRy, yRz e $x \not R z$. Assim, por exemplo, a relação $R = \{(a, a), (a, b), (b, c), (c, c)\}$ sobre $E = \{a, b, c\}$ não é transitiva pois aRb, bRc e $a \not R c$.

d) Anti-simétrica

Dizemos que R é anti-simétrica quando está satisfeita a condição:

$(\forall x, y \in E)\ (xRy \text{ e } yRx \implies x = y)$

ou, a equivalente:

$(\forall x, y \in E)\ (x \neq y \implies x \not R y \text{ ou } y \not R x)$

isto é, se x e y são elementos distintos, então x não se relaciona com y ou y não se relaciona com x.

Exemplos

1º) A relação $R = \{(a, a), (b, b), (a, b), (a, c)\}$ sobre $E = \{a, b, c\}$ é anti-simétrica.

2º) A relação R de divisibilidade sobre $\mathbb{N}$:

$xRy \iff x \mid y$ (lê-se: "x é divisor de y")

é anti-simétrica pois, dados dois números naturais x e y, se $x \mid y$ e $y \mid x$ então $x = y$.

3º) A relação R sobre $\mathbb{R}$ dada por $xRy \iff x \leqslant y$ é anti-simétrica pois, sendo x e y números reais quaisquer, se $x \leqslant y$ e $y \leqslant x$ então $x = y$.

Contra-exemplo

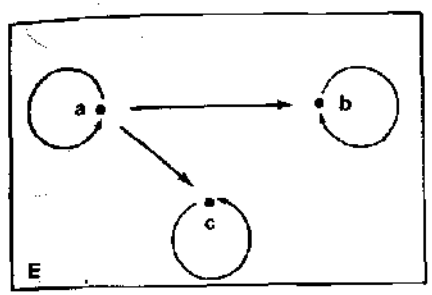
Notemos que uma relação R sobre E *não* é anti-simétrica se existirem $x, y \in E$ tais que $x \neq y$, xRy e yRx. Assim, por exemplo, a relação $R = \{(a, a), (a, b), (b, a), (b, b), (c, c)\}$ sobre $E = \{a, b, c\}$ não é anti-simétrica pois $a \neq b$, aRb e bRa.

Nota: Se E é finito, com "poucos" elementos, é possível visualizar se as propriedades definidas se verificam ou não para uma relação R, através de um esquema de flechas, do seguinte modo:

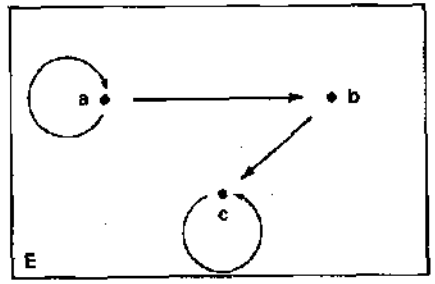
Reflexiva

Em cada ponto do diagrama deve haver um laço.

Exemplo



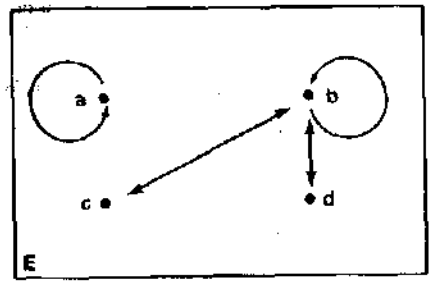
Contra-exemplo



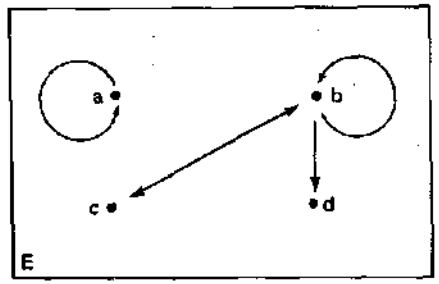
Simétrica

Toda flecha deve ter duas "pontas".

Exemplo



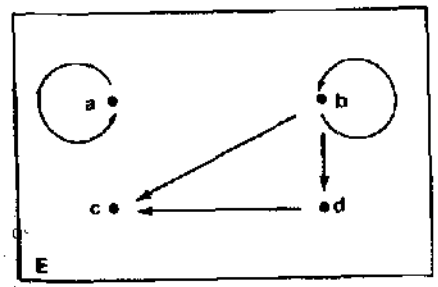
Contra-exemplo



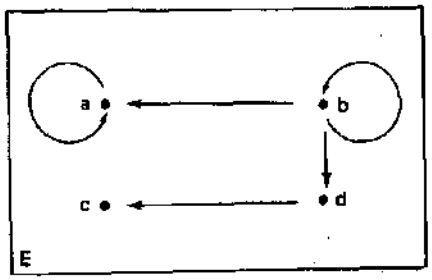
Transitiva

Para todo par de flechas consecutivas existe uma flecha cuja origem é a da primeira e a extremidade, a da segunda.

Exemplo



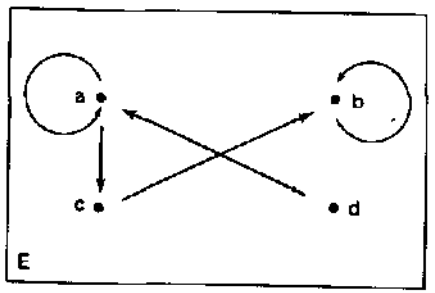
Contra-exemplo



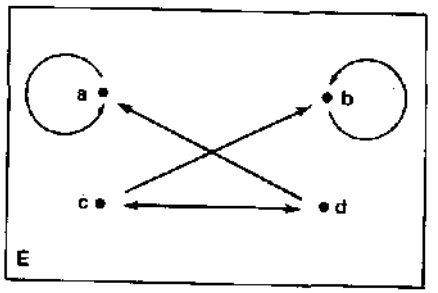
Anti-simétrica

Não há flechas de duas pontas.

Exemplo



Contra-exemplo

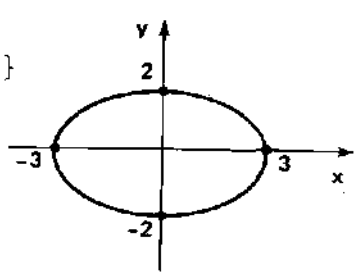


EXERCÍCIOS

1. Sejam $A = \{0, 2, 4, 6, 8\}$ e $B = \{1, 3, 5, 9\}$. Enumerar os elementos das seguintes relações $R_1 = \{(x, y) \in A \times B \mid y = x + 1\}$ e $R_2 = \{(x, y) \in A \times B \mid x \leqslant y\}$. Dizer qual é o domínio, a imagem e a inversa de cada.

2. A é um conjunto com 5 elementos e $R = \{(0,1); (1, 2); (2, 3); (3, 4)\}$ é uma relação sobre A. Pede-se obter:
   I) os elementos de A;
   II) domínio e imagem de R;
   III) os elementos, domínio e imagem de R^{-1};
   IV) os gráficos de R e R^{-1}.

3. Seja $R = \{(x, y) \mid x \in \mathbb{R},\ y \in \mathbb{R},\ 4x^2 + 9y^2 = 36\}$
   Segue-se o esboço de R no diagrama coordenado de $\mathbb{R} \times \mathbb{R}$:



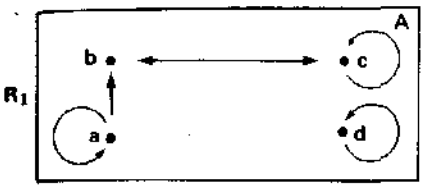
   Achar:
   (1) o domínio de R;
   (2) a imagem de R;
   (3) R^{-1}.

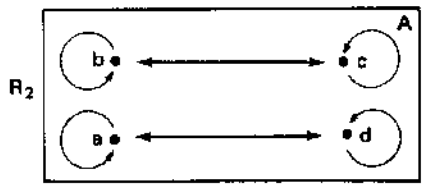
4. Seja R a relação nos números $\mathbb{N}^* = \{1, 2, 3, \ldots\}$ definida pela sentença aberta "$2x + y = 10$", isto é, seja $R = \{(x, y) \mid x \in \mathbb{N}^*,\ y \in \mathbb{N}^*,\ 2x + y = 10\}$.
   Achar:
   (1) o domínio de R. (2) a imagem de R. (3) R^{-1}.

5. Sejam A e B dois conjuntos com m e n elementos, respectivamente. Calcular o número de elementos de $A \times B$ e os números de relações de A em B.

6. Seja R a relação em $A = \{1, 2, 3, 4, 5\}$ tal que:
   $x\ R\ y \iff (x - y$ é múltiplo de 2).
   Enumerar os elementos de R. Que propriedades R apresenta?
   Sugestão: fazer o diagrama de flechas.

7. Enumerar os elementos das seguintes relações em $A = \{a, b, c, d\}$
   Que propriedades R_1 e R_2 apresentam?





8. Um casal tem 5 filhos: álvaro, bruno, cláudio, dario e elizabete. Enumerar os elementos da relação R definida no conjunto $E = \{a, b, c, d, e\}$ por $xRy \iff x$ é irmão de y. Que propriedades R apresenta?
   Nota: x é irmão de y quando x é homem, $x \neq y$ e x e y têm os mesmos pais.

9. Seja A o conjunto das retas definidas pelos vértices de um paralelogramo abcd. Enumerar os elementos da relação R em A assim definida: $x\ R\ y \iff x \parallel y$.
   Quais são as propriedades apresentadas por R?
   Nota: x é paralela a y quando $x = y$ ou $x \cap y = \phi$ com x e y coplanares.

10. Determinar todas as relações binárias sobre o conjunto $A = \{a, b\}$.
    Quais são reflexivas? E simétricas? E transitivas? E anti-simétricas?
    Sugestão: examine cada subconjunto de $A \times A$.

11. Seja $A = \{1, 2, 3\}$. Considerem-se as seguintes relações em A:
    $R_1 = \{(1, 2); (1, 1); (2, 2); (2\ 1); (3, 3)\}$
    $R_2 = \{(1, 1); (2, 2); (3, 3); (1, 2); (2, 3)\}$
    $R_3 = \{(1, 1); (2, 2); (1, 2); (2, 3); (3, 1)\}$
    $R_4 = A \times A$
    $R_5 = \phi$
    Quais são reflexivas? simétricas? transitivas? anti-simétricas?

12. Construir sobre o conjunto $E = \{a, b, c, d\}$ relações R_1, R_2, R_3 e R_4 tais que R_1 só tem a propriedade reflexiva, R_2 só a simétrica, R_3 só a transitiva e R_4 só a anti-simétrica.
    Sugestão: faça o diagrama de flechas.

13. Pode uma relação sobre um conjunto $E \neq \phi$ ser simétrica e anti-simétrica? Pode uma relação sobre E não ser simétrica nem anti-simétrica? Justifique.

14. Seja R uma relação em $\mathbb{R}$ (conjunto dos números reais) e seja G_r seu gráfico cartesiano. Qual é a particularidade apresentada por G_r quando:
    a) R é reflexiva? b) R é simétrica?

15. Esboçar os gráficos cartesianos das seguintes relações em $\mathbb{R}$:

$R_1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$

$R_2 = \{(x, y) \in \mathbb{R}^2 \mid x + y \leqslant 2\}$

$R_3 = \{(x, y) \in \mathbb{R}^2 \mid y^2 = x\}$

$R_4 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leqslant 4\}$

$R_5 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + x = y^2 + y\}$

$R_6 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 < 16 \quad (\text{ou } x^2 + y^2 - 16 < 0)\}$

$R_7 = \{(x, y) \in \mathbb{R}^2 \mid x^2 - 4y^2 \geqslant 9 \quad (\text{ou } x^2 - 4y^2 - 9 \geqslant 0)\}$

$R_8 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \geqslant 16\}$

$R_9 = \{(x, y) \in \mathbb{R}^2 \mid x^2 - 4y^2 < 9\}$

$R_{10} = \{(x, y) \in \mathbb{R}^2 \mid y = x^2\}$

$R_{11} = \{(x, y) \in \mathbb{R}^2 \mid y \leqslant x^2\}$

$R_{12} = \{(x, y) \in \mathbb{R}^2 \mid y < 3 - x\}$

$R_{13} = \{(x, y) \in \mathbb{R}^2 \mid y \geqslant \operatorname{sen} x\}$

$R_{14} = \{(x, y) \in \mathbb{R}^2 \mid y \geqslant x^3\}$

$R_{15} = \{(x, y) \in \mathbb{R}^2 \mid y > x^3\}$

Quais são reflexivas?
Quais são simétricas?

16. Seja A um conjunto finito com n elementos.
Quantas são as relações binárias em A?
Quantas são as relações reflexivas em A?
Quantas são as relações simétricas em A?

17. Provar que se uma relação R é transitiva, então R^{-1} também o é.

18. Sejam R e S relações no mesmo conjunto A. Provar que:

a) $R^{-1} \cap S^{-1} = (R \cap S)^{-1}$

b) $R^{-1} \cup S^{-1} = (R \cup S)^{-1}$

c) Se R e S são transitivas, então $R \cap S$ é transitiva

d) Se R e S são simétricas, então $R \cup S$ e $R \cap S$ são simétricas

e) Para todo R, $R \cup R^{-1}$ é simétrica.

19. Seja R uma relação de E em F e S uma relação de F em G. Chama-se *relação composta* de R e S a seguinte relação (indicada SoR) de E em G:

$SoR = \{(x, z) \in E \times G \mid \exists\, y \in F : (x, y) \in R \text{ e } (y, z) \in S\}$.

Mostre que:

a) $(SoR)^{-1} = R^{-1} o\, S^{-1}$

b) Se R é reflexiva, então RoR^{-1} e $R^{-1} o\, R$ também o são ($R \subset E \times E$).

c) Se R é uma relação sobre E, então RoR^{-1} e $R^{-1} o\, R$ são simétricas.

d) Se R e S são relações simétricas sobre um conjunto E, então:

SoR é simétrica $\iff$ SoR = RoS.

§ 2º — RELAÇÕES DE EQUIVALÊNCIA

1. DEFINIÇÃO

Definição 7: Uma relação R sobre um conjunto E não vazio é chamada *relação de equivalência sobre E* se, e somente se, R é reflexiva, simétrica e transitiva, isto é, se são verdadeiras as sentenças:

i) $(\forall x)\ (x \in E \implies xRx)$

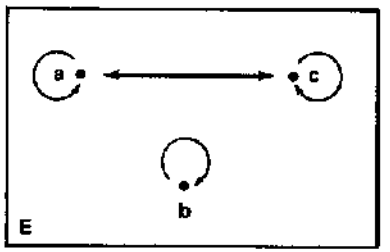
ii) $(\forall x\ \forall y)\ (xRy \implies yRx)$

iii) $(\forall x\ \forall y\ \forall z)\ (xRy \text{ e } yRz \implies xRz)$

Quando R é uma relação de equivalência sobre E, para exprimirmos que $(a, b) \in R$ usaremos a notação $a \equiv b\ (R)$, que se lê: "*a* é equivalente a *b* módulo R".

2. EXEMPLOS

1º) A relação
$R = \{(a, a), (b, b), (c, c), (a, c), (c, a)\}$
é uma relação de equivalência sobre
$E = \{a, b, c\}$.



2º) A relação de igualdade sobre $\mathbb{R}$:

$xRy \iff x = y$

é uma relação de equivalência pois:

$(\forall x)\ (x \in \mathbb{R} \implies x = x)$

$(\forall x\ \forall y)\ (x = y \implies y = x)$

$(\forall x\ \forall y\ \forall z)\ (x = y \text{ e } y = z \implies x = z)$

3º) A relação de congruência módulo m (onde $m \in \mathbb{Z}$ e $m > 1$) sobre $\mathbb{Z}$, conforme foi visto no item 8 do capítulo zero.

4º) A relação de paralelismo definida para as retas de um espaço euclidiano:

$xRy \iff x \parallel y$

é uma relação de equivalência, pois, se x, y, z são retas do espaço, temos:

i) $x \parallel x$

ii) $x \parallel y \implies y \parallel x$

iii) $(x \parallel y \text{ e } y \parallel z) \implies x \parallel z$

3. CLASSES DE EQUIVALÊNCIA

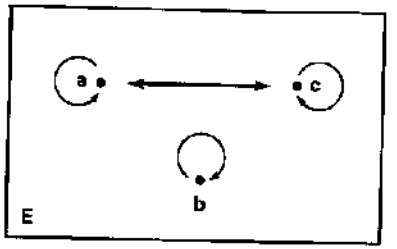
Definição 8: Seja R uma relação de equivalência sobre E. Dado $a \in E$, chama-se *classe de equivalência determinada por a, módulo R,* o subconjunto $\bar{a}$ de E constituído pelos elementos x tais que xRa. Em símbolos:

$$\bar{a} = \{x \in E \mid xRa\}$$

Definição 9: O conjunto das classes de equivalência módulo R será indicado por E/R e chamado *conjunto quociente de E por R.*

Exemplos

1º) Na relação de equivalência
$R = \{(a, a), (b, b), (c, c), (a, c), (c, a)\}$
temos:
$\bar{a} = \{a, c\}$
$\bar{b} = \{b\}$
$\bar{c} = \{c, a\}$
$E/R = \{\{a, c\}, \{b\}\}$



2º) A relação de congruência módulo m sobre $\mathbb{Z}$:

$$xRy \iff x \equiv y \pmod{m}$$

onde $m \in \mathbb{Z}$ e $m > 1$, determina em $\mathbb{Z}$ um conjunto quociente $\mathbb{Z}/R$ que será indicado por $\mathbb{Z}_m$.

Vamos provar que $\mathbb{Z}_m$ tem exatamente m elementos, isto é, $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1}\}$.

i) Dado $a \in \mathbb{Z}$, efetuemos a divisão euclidiana de a por m. Sendo q o quociente e r o resto dessa divisão, temos:

$$a = mq + r \quad (0 \leqslant r < m)$$

logo, $a - r = mq$, isto é, $a \equiv r \pmod{m}$, ou ainda, $\bar{a} = \bar{r}$.

Como $r \in \{0, 1, 2, \ldots, m-1\}$, temos que

$$\bar{a} \in \mathbb{Z}_m \implies \bar{a} \in \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1}\}$$

ii) Suponhamos agora que existam duas classes iguais em $\{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1}\}$, isto é:

$$\bar{r} = \bar{s} \text{ com } 0 \leqslant r < s < m$$

Neste caso, temos:

$\bar{r} = \bar{s} \Rightarrow r \equiv s \pmod{m} \implies m \mid s - r$

Como $0 < s - r < m$ isto é impossível.

Logo o número de elementos de $\mathbb{Z}_m$ é exatamente m.

Teorema 1: Seja R uma relação de equivalência sobre E e sejam $a \in E$ e $b \in E$. As seguintes proposições são equivalentes:

(I) aRb; (II) $a \in \bar{b}$; (III) $b \in \bar{a}$; (IV) $\bar{a} = \bar{b}$

Demonstração

(I) $\implies$ (II): decorre da definição de classe de equivalência

(II) $\implies$ (III): $a \in \bar{b} \implies aRb \implies bRa \implies b \in \bar{a}$

(III) $\implies$ (IV): da hipótese $b \in \bar{a}$ decorre bRa e, pela propriedade simétrica, decorre aRb. Provemos que $\bar{a} \subset \bar{b}$ e $\bar{b} \subset \bar{a}$. Dado $x \in \bar{a}$, temos:

$$\left.\begin{array}{l} x \in \bar{a} \implies xRa \\ \text{por hipótese } aRb \end{array}\right\} \implies xRb \implies x \in \bar{b}$$

então $\bar{a} \subset \bar{b}$.

Dado um $x \in \bar{b}$, temos:

$$\left.\begin{array}{l} x \in \bar{b} \implies xRb \\ \text{por hipótese } bRa \end{array}\right\} \implies xRa \implies x \in \bar{a}$$

então $\bar{b} \subset \bar{a}$.

(IV) $\implies$ (I): como $a \in \bar{a}$ e $b \in \bar{b}$, não são vazios os conjuntos $\bar{a}$ e $\bar{b}$. Seja $x \in \bar{a} = \bar{b}$. Temos:

$$\left.\begin{array}{l} x \in \bar{a} \implies xRa \implies aRx \\ x \in \bar{b} \implies xRb \end{array}\right\} \implies aRb \qquad \blacksquare$$

4. PARTIÇÃO DE UM CONJUNTO

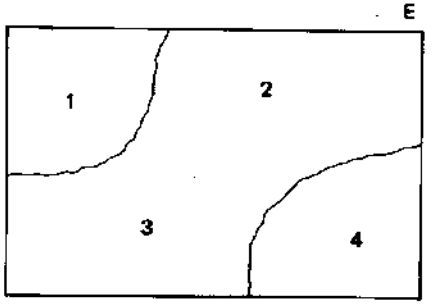
Definição 10: Seja E um conjunto não vazio. Diz-se que uma classe $\mathscr{T}$ de subconjuntos não vazios de E é uma *partição de E* se, e somente se:

a) dois membros quaisquer de $\mathscr{T}$ ou são iguais ou são disjuntos;

b) a união dos membros de $\mathscr{T}$ é igual a E.

Exemplos

1º) $\mathscr{T} = \{\{1\}, \{2, 3\}, \{4\}\}$ é uma partição do conjunto $E = \{1, 2, 3, 4\}$.

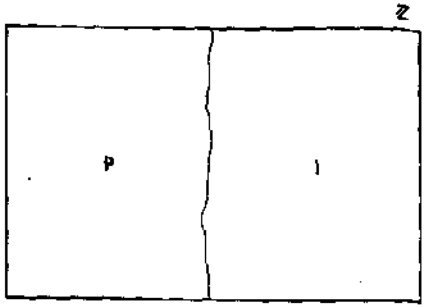


2º) Sejam

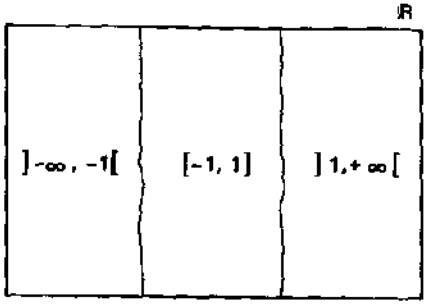
$P = \{x \in \mathbb{Z} \mid x \text{ é par}\}$

$I = \{x \in \mathbb{Z} \mid x \text{ é impar}\}$

então $\mathcal{S} = \{P, I\}$ é uma partição de $\mathbb{Z}$.



3º) $\mathcal{T} = \{\,]-\infty, -1[\,, [-1, 1],]1, +\infty[\,\}$ é uma partição de $\mathbb{R}$.



Provaremos a seguir que, através de uma relação de equivalência sobre um conjunto E, fica determinada uma partição de E e vice-versa. Certos conceitos matemáticos como os de número inteiro, número racional, número real, vetor, etc., são fixados através de relações de equivalência e classes de equivalência cuja construção se baseia nos teoremas seguintes.

Teorema 2: Se R é uma relação de equivalência sobre um conjunto E, então E/R é uma partição de E.

Demonstração

a) Seja $\bar{a} \in E/R$. Como a relação R é reflexiva, então aRa, portanto, $a \in \bar{a}$. Assim, $\bar{a} \neq \phi$ para todo $a \in E$.

b) Sejam $\bar{a} \in E/R$ e $\bar{b} \in E/R$ tais que $\bar{a} \cap \bar{b} \neq \phi$. Provaremos que $\bar{a} = \bar{b}$. De fato, seja $y \in \bar{a} \cap \bar{b}$; então:

$$\left.\begin{array}{l} y \in \bar{a} \implies yRa \implies aRy \\ y \in \bar{b} \implies yRb \end{array}\right\} \implies aRb \implies \bar{a} = \bar{b}$$

c) Provemos que $\bigcup_{a \in E} \bar{a} = E$.

I) Para cada $a \in E$, temos $\bar{a} \subset E$, portanto, $\bigcup_{a \in E} \bar{a} \subset E$.

II) Sendo x um elemento qualquer de E, temos:

$$x \in E \implies xRx \implies x \in \bar{x} \implies x \in \bigcup_{a \in E} \bar{a}.$$

Assim, $E \subset \bigcup_{a \in E} \bar{a}$ ∎

Teorema 3: Se $\mathcal{T}$ é uma partição de E, então existe uma relação R de equivalência sobre E de modo que $E/R = \mathcal{T}$.

Demonstração: Seja R a relação sobre E assim definida:

$$xRy \iff \exists\, A \in \mathcal{T} : x \in A \text{ e } y \in A$$

isto é, x está na relação com y quando existe um conjunto A da partição $\mathcal{T}$ que contém x e y.

Temos:

(i) Para todo x em E, existe uma classe A em $\mathcal{T}$ tal que $x \in A$, portanto, xRx.

(ii) Sendo $x \in E$ e $y \in E$, vem:

$$xRy \implies \exists\, A \in \mathcal{T} : x, y \in A \implies y, x \in A \implies yRx$$

(iii) Sendo $x, y, z \in E$, vem:

$$xRy \implies \exists\, A_1 \in \mathcal{T} : x, y \in A_1$$
$$yRz \implies \exists\, A_2 \in \mathcal{T} : y, z \in A_2$$

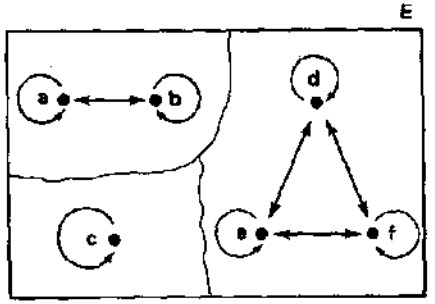
Como $A_1 \cap A_2 \neq \phi$, então $A_1 = A_2$, portanto $x, z \in A_1 = A_2 \in \mathcal{T}$ e, assim, xRz. ∎

Exemplo

Dada a partição

$\mathcal{T} = \{\{a, b\}, \{c\}, \{d, e, f\}\}$

de $E = \{a, b, c, d, e, f\}$, a ela podemos associar a relação de equivalência



$R = \{(a, a), (a, b), (b, a), (b, b), (c, c), (d, d), (d, e), (e, d), (e, e), (e, f), (f, e), (f, f), (f, d), (d, f)\}$.

e temos $E/R = \{\{a, b\}, \{c\}, \{d, e, f\}\} = \mathcal{T}$

EXERCÍCIOS

20. Quais das relações abaixo são relações de equivalência sobre $E = \{a, b, c\}$?

$R_1 = \{(a, a), (a, b), (b, a), (b, b), (c, c)\}$

$R_2 = \{(a, a), (a, b), (b, a), (b, b), (b, c)\}$

$R_3 = \{(a, a), (b, b), (b, c), (c, b), (a, c), (c, a)\}$

$R_4 = E \times E$

$R_5 = \phi$

21. Quais das seguintes sentenças abertas definem uma relação de equivalência em $\mathbb{N}$ (conjunto dos números naturais)?

a) $xRy \iff \exists\ k \in \mathbb{Z} \mid x - y = 3k$

b) $x \mid y$

c) $x \leqslant y$

d) $mdc\ (x, y) = 1$

e) $x + y = 10$

22. Seja A o conjunto dos triângulos do espaço euclidiano. Seja R a relação em A definida por:

$xRy \iff x$ é semelhante a y. Mostrar que R é de equivalência.

23. Seja A o conjunto das retas de um plano α e seja P um ponto fixo de α. Quais das relações abaixo definidas são relações de equivalência em A?

a) $xRy \iff x \mathbin{/\!/} y$

b) $xRy \iff x \perp y$

c) $xRy \iff P \in x \cap y$

24. Mostrar que a relação R sobre $\mathbb{N} \times \mathbb{N}$ tal que $(a, b)\ R\ (c, d) \iff a + b = c + d$ é uma relação de equivalência.

25. Mostrar que a relação S sobre $\mathbb{Z} \times \mathbb{Z}^*$ tal que $(a, b)\ S\ (c, d) \iff ad = bc$ é uma relação de equivalência.

26. Seja E um conjunto não vazio. Dados $X, Y \in \mathcal{P}(E)$ (conjunto das partes de E) mostre que as relações R e S são de equivalência em $\mathcal{P}(E)$:

a) $X\,R\,Y \iff X \cap A = Y \cap A$

b) $X\,S\,Y \iff X \cup A = Y \cup A$

onde A é um subconjunto fixo de E.

27. Seja $A = \{x \in \mathbb{Z} \mid 0 \leqslant x \leqslant 10\}$ e R a relação sobre A definida por $xRy \iff \exists\ k \in \mathbb{Z} \mid x - y = 4k$. Determinar o conjunto-quociente A/R.

28. Seja $A = \{x \in \mathbb{Z} \mid \mid x \mid \leqslant 5\}$ e R a relação sobre A definida por $xRy \iff x^2 + 2x = y^2 + 2y$. Determinar o conjunto-quociente A/R.

29. Sejam $E = \{-3, -2, -1, 0, 1, 2, 3\}$ e $R = \{(x, y) \in E \times E \mid x + |x| = y + |y|\}$. Mostrar que R é uma relação de equivalência e descrever E/R.

30. Seja R a relação sobre $\mathbb{Q}$ definida da forma seguinte $xRy \iff x - y \in \mathbb{Z}$. Provar que R é uma relação de equivalência e descrever a classe $\overline{1}$.

31. Seja $R = \{(x, y) \in \mathbb{R}^2 \mid x - y \in \mathbb{Q}\}$. Provar que R é uma relação de equivalência e descrever as classes representadas por $1/2$ e $\sqrt{2}$.

32. Mostrar que a relação S sobre $\mathbb{C}$ (conjunto dos números complexos) definida pela lei:

$$(x + yi)\ S\ (z + ti) \iff x^2 + y^2 = z^2 + t^2$$

com $x, y, z, t \in \mathbb{R}$, é uma relação de equivalência. Descrever a classe $\overline{1 + i}$.

33. Mostre que é uma relação de equivalência em $\mathbb{C}$:

$R = \{(a + bi, c + di) \mid b = d\}$. Descreva o conjunto-quociente $\mathbb{C}/R$.

34. Sejam $P = (x_1, y_1)$ e $Q = (x_2, y_2)$ pontos genéricos de um plano cartesiano π. Mostre que as relações a seguir são relações de equivalência sobre π e interprete geometricamente as classes de equivalência e o conjunto-quociente, em cada caso.

a) $P\,R\,Q \iff x_1 y_1 = x_2 y_2$

b) $P\,S\,Q \iff y_2 - y_1 = x_2 - x_1$

c) $P\,T\,Q \iff x_1^2 + y_1^2 = x_2^2 + y_2^2$

d) $P\,V\,Q \iff k_1 x_1^2 + k_2 y_1^2 = k_1 x_2^2 + k_2 y_2^2$, com $k_2 > k_1 > 0$.

35. Qual é a relação de equivalência associada a cada uma das seguintes partições?

I) $A/R = \{\{a, b\}, \{c, d, e\}\}$

II) $A/R = \{\{a, b, c\}, \{d\}, \{e\}\}$

III) $A/R = \{\{0, \pm 2, \pm 4, \ldots\}, \{\pm 1, \pm 3, \pm 5, \ldots\}\}$

36. Quais são as relações de equivalência sobre $E = \{a, b\}$?

37. Enumerar todas as relações de equivalência sobre $A = \{a, b, c\}$.

38. Quantas são as relações de equivalência que podem ser estabelecidas sobre $E = \{a, b, c, d\}$?

39. Seja R uma relação reflexiva sobre um conjunto E. Mostre que R é uma relação de equivalência se, e somente se, $RoR^{-1} = R$.

Sugestão: lembre do exercício 19 deste capítulo.

40. Seja R uma relação reflexiva sobre um conjunto E com as seguintes propriedades:

1) $D(R) = E$;

2) $(\forall\ a, b, c \in E)\ (aRc \text{ e } bRc \implies aRb)$.

Mostre que R é uma relação de equivalência.

§ 3º — RELAÇÕES DE ORDEM

1. DEFINIÇÕES

Definição 11: Uma relação R sobre um conjunto E não vazio é chamada *relação de ordem parcial sobre E* se, e somente se, R é reflexiva, anti-simétrica e transitiva, isto é, são verdadeiras as sentenças:

i) $(\forall x)\ (x \in E \Longrightarrow xRx)$

ii) $(\forall x, y \in E)\ (xRy \text{ e } yRx \Longrightarrow x = y)$

iii) $(\forall x, y, z \in E)\ (xRy \text{ e } yRz \Longrightarrow xRz)$

Quando R é uma relação de ordem parcial sobre E, para exprimirmos que $(a, b) \in R$ usaremos a notação $a \preccurlyeq b\ (R)$, que se lê: "a precede b na relação R".

Para exprimirmos que $(a, b) \in R$ e $a \neq b$ usaremos a notação $a \prec b\ (R)$, que se lê: "a precede estritamente b na relação R".

Quando não houver dúvidas quanto à relação de ordem que está sendo considerada, escreveremos apenas $a \preccurlyeq b$ ("a precede b") para indicar $(a, b) \in R$ e $a \prec b$ ("a precede estritamente b") para indicar $(a, b) \in R$ e $a \neq b$.

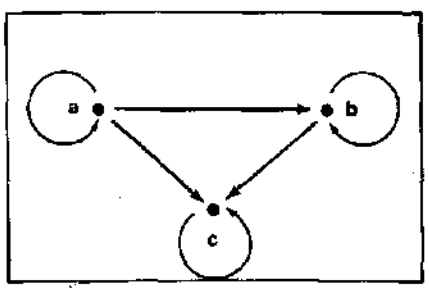
Definição 12: Um *conjunto parcialmente ordenado* é um conjunto sobre o qual se definiu uma certa relação de ordem parcial.

Definição 13: Seja R uma relação de ordem parcial sobre E. Os elementos $a, b \in E$ se dizem *comparáveis mediante R* se $a \preccurlyeq b$ ou $b \preccurlyeq a$.

Definição 14: Se dois elementos quaisquer de E forem comparáveis mediante R, então R será chamada *relação de ordem total sobre E*. O conjunto E, neste caso, é chamado *conjunto totalmente ordenado.*

2. EXEMPLOS

1º) A relação $R = \{(a, a), (b, b), (c, c), (a, b), (b, c), (a, c)\}$ é uma relação de ordem total sobre $E = \{a, b, c\}$, conforme se pode notar no diagrama ao lado. Observe-se que o fato de não haver dois pontos que não estejam ligados por uma flecha indica que a ordem é total.



2º) A relação R sobre $\mathbb{R}$ definida por $xRy \Longleftrightarrow x \leqslant y$ (menor que ou igual) é uma relação de ordem total, denominada ordem habitual, pois:

$(\forall x)\ (x \in \mathbb{R} \Longrightarrow x \leqslant y)$

$(\forall x, y \in \mathbb{R})\ (x \leqslant y \text{ e } y \leqslant x \Longrightarrow x = y)$

$(\forall x, y, z \in \mathbb{R})\ (x \leqslant y \text{ e } y \leqslant z \Longrightarrow x \leqslant z)$

$(\forall x, y)\ (x, y \in \mathbb{R} \Longrightarrow x \leqslant y \text{ ou } y \leqslant x)$

3º) A relação R de divisibilidade sobre $\mathbb{N}$: $xRy \Longleftrightarrow x \mid y$ é uma relação de ordem parcial pois:

$(\forall x)\ (x \in \mathbb{N} \Longrightarrow x \mid x)$

$(\forall x, y \in \mathbb{N})\ (x \mid y \text{ e } y \mid x \Longrightarrow x = y)$

$(\forall x, y, z \in \mathbb{N})\ (x \mid y \text{ e } y \mid z \Longrightarrow x \mid z)$

como se pode provar facilmente, usando a noção de divisor.

4º) A relação de inclusão sobre uma família $\mathcal{F}$ de subconjuntos de um dado conjunto é uma relação de ordem pois:

$(\forall x)\ (x \in \mathcal{F} \Longrightarrow x \subset x)$

$(\forall x, y \in \mathcal{F})\ (x \subset y \text{ e } y \subset x \Longrightarrow x = y)$

$(\forall x, y, z \in \mathcal{F})\ (x \subset y \text{ e } y \subset z \Longrightarrow x \subset z)$

3. LIMITES SUPERIORES E INFERIORES

Seja E um *conjunto parcialmente* ordenado mediante a relação $\preccurlyeq$. Seja A um subconjunto de E, com $A \neq \phi$.

Definição 15: Um elemento $L \in E$ é um *limite superior* de A se for verdadeira a proposição:

$$(\forall x)\ (x \in A \Longrightarrow x \preccurlyeq L)$$

isto é, quando qualquer elemento de A precede L.

Definição 16: Um elemento $\ell \in E$ é um *limite inferior* de A se for verdadeira a proposição:

$$(\forall x)\ (x \in A \Longrightarrow \ell \preccurlyeq x)$$

isto é, quando ℓ precede qualquer elemento de A.

4. MÁXIMO E MÍNIMO

Seja A um subconjunto não vazio do conjunto E parcialmente ordenado pela relação $\preccurlyeq$

Definição 17: Um elemento $M \in A$ é um *máximo* de A quando se verifica a seguinte propriedade:

$$(\forall x)\ (x \in A \Longrightarrow x \preccurlyeq M)$$

isto é, quando M é um limite superior de A e pertence a A.

Definição 18: Um elemento $m \in A$ é um mínimo de A quando se verifica a seguinte propriedade:

$$(\forall x)\ (x \in A \Longrightarrow m \preccurlyeq x)$$

isto é, quando m é um limite inferior de A e pertence a A.

Proposição 1: Se A é um subconjunto do conjunto parcialmente ordenado E e existe um máximo (mínimo) de A, então ele é único.

Demonstração: Faremos a demonstração apenas no que tange ao máximo. Admitamos que M_1 e M_2 sejam máximos de A. Temos:

M_1 é máximo de A e $M_2 \in A \Longrightarrow M_2 \preccurlyeq M_1$

M_2 é máximo de A e $M_1 \in A \Longrightarrow M_1 \preccurlyeq M_2$

então $M_1 = M_2$. ■

5. SUPREMO E ÍNFIMO

Definição 19: Seja A um subconjunto não vazio do conjunto parcialmente ordenado E. Chama-se *supremo* de A o mínimo (caso exista) do conjunto dos limites superiores de A. Chama-se *ínfimo* de A o máximo (caso exista) do conjunto dos limites inferiores de A.

6. ELEMENTOS MAXIMAIS E MINIMAIS

Seja A um subconjunto não vazio do conjunto parcialmente ordenado E.

Definição 20: Um elemento $m_1 \in A$ é um *elemento maximal* de A quando se verifica:

$$(\forall x \in A)\ (m_1 \preccurlyeq x \Longrightarrow m_1 = x)$$

isto é, quando o único elemento de A precedido por m_1 é ele próprio.

Definição 21: Um elemento $m_0 \in A$ é um *elemento minimal* de A quando se verifica:

$$(\forall x \in A)\ (x \preccurlyeq m_0 \Longrightarrow x = m_0)$$

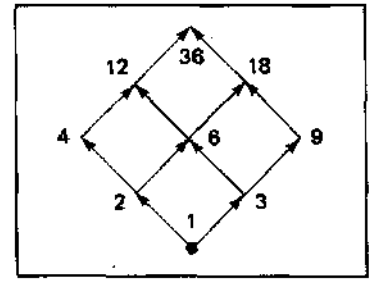
isto é, quando o único elemento de A que precede m_0 é ele próprio.

7. EXEMPLOS

1º) Se $E = \mathbb{R}$, $A =]0, 1]$ e a ordem é a habitual, temos:

a) são limites superiores de A os números $L \geqslant 1$;
b) são limites inferiores de A os números $\ell \leqslant 0$;
c) o máximo de A é 1;
d) A não tem mínimo;
e) o supremo de A é 1;
f) o ínfimo de A é 0;
g) só 1 é elemento maximal de A;
h) A não tem elementos minimais.

2º) Se $E = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$, $A = \{2, 4, 6\}$ e a ordem é a divisibilidade, o diagrama simplificado *(omitindo as propriedades reflexiva e transitiva)* ao lado mostra que:



a) os limites superiores de A são: 12 e 36;
b) os limites inferiores de A são: 1 e 2;
c) A tem mínimo 2 e não tem máximo;
d) A tem ínfimo 2 e supremo 12;
e) *só 2 é elemento minimal de A;*
f) os elementos maximais de A são 4 e 6.

Nota: É costume dar uma relação de ordem parcial sobre um conjunto finito, com "poucos" elementos, por meio de um *diagrama simplificado* como o do exemplo acima, omitindo as propriedades reflexiva e transitiva, para não sobrecarregar o esquema de flechas.

EXERCÍCIOS

Nota: Aqui o símbolo $\leqslant$ quando não definido explicitamente, indica a relação de ordem habitual seja em **N**, **Z**, **Q** ou **IR**.

41. Fazer um diagrama simplificado das seguintes ordens no conjunto $A = \{1, 2, 3, 4, 6, 12\}$
a) ordem habitual b) ordem por divisibilidade.

42. Dizer se cada um dos seguintes subconjuntos de $\mathbb{N}$ é ou não totalmente ordenado pela relação de divisibilidade:

a) $\{24, 2, 6\}$ b) $\{3, 15, 5\}$ c) $\{15, 5, 30\}$ d) $\mathbb{N}$

43. Fazer um diagrama simplificado da relação de ordem por inclusão em $E = \mathscr{P}(\{a, b\})$ e em $E' = \mathscr{P}(\{a, b, c\})$.

44. Seja $\mathbb{C}$ o conjunto dos números complexos e sejam $x = a + bi$ e $y = c + di$ dois elementos de $\mathbb{C}$. Mostrar que R é relação de ordem parcial em $\mathbb{C}$:

$$xRy \iff a \leqslant c \text{ e } b \leqslant d$$

45. Fazer um diagrama simplificado da relação de ordem por divisibilidade em $A = \{2, 3, 5, 6, 10, 15, 30\}$. Quais os limites superiores, limites inferiores, ínfimo, supremo, máximo e mínimo, elementos maximais e minimais de $B = \{6, 10\}$?

46. Fazer um diagrama simplificado da relação de ordem por inclusão em:

$E = \{\{a\}, \{b\}, \{a, b, c\}, \{a, b, d\}, \{a, b, c, d\}, \{a, b, c, d, e\}\}$

Quais são os limites superiores, limites inferiores, ínfimo, supremo, máximo e mínimo do subconjunto $A = \{\{a, b, c\}, \{a, b, d\}, \{a, b, c, d\}\}$ de E?

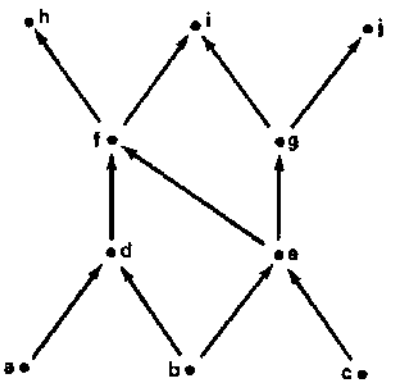
47. Seja $A = \{x \in \mathbb{Q} \mid 0 \leqslant x^2 \leqslant 2\}$ um subconjunto de $\mathbb{Q}$, onde está definida a relação de ordem habitual. Determinar os limites superiores, limites inferiores, ínfimo, supremo, máximo e mínimo de A.

48. Ao lado está o diagrama simplificado da relação de ordem R sobre $E = \{a, b, c, d, e, f, g, h, i, j\}$.

Pede-se:

a) Determinar os limites superiores, os limites inferiores, o ínfimo, o supremo, o máximo e o mínimo de $A = \{d, e\}$.

b) Dar os pares que constituem R^{-1}.



49. Em $\mathbb{N} \times \mathbb{N}$ define-se $(a, b) \leqslant (c, d) \iff a \mid c \text{ e } b \leqslant d$.

a) mostrar que esta relação ($\leqslant$) é uma relação de ordem parcial em $\mathbb{N} \times \mathbb{N}$.

b) Sendo $A = \{(2, 1); (1, 2)\}$, ache os limites superiores, limites inferiores, ínfimo, supremo, máximo e mínimo de A.

50. Provar que se R é uma relação de ordem sobre E, então R^{-1} também é.

Nota: R^{-1} é, neste caso, a *ordem oposta* de R.

51. Mostre que é uma relação de ordem total no conjunto $\mathbb{C}$:

$R = \{(a + bi,\ c + di) \in \mathbb{C}^2 \mid a < c \text{ ou } (a = c \text{ e } b \leqslant d)\}$

Nota: esta relação é denominada *ordem lexicográfica*.

§ 4º — APLICAÇÕES

1. CONCEITO

Definição 22: Seja f uma relação de E em F. Dizemos que f é uma *aplicação* de E em F se:

a) $D(f) = E$;

b) Dado $a \in D(f)$, é único o elemento $b \in F$ de modo que $(a, b) \in f$.

Se f é uma aplicação de E em F, escrevemos $b = f(a)$ (lê-se: b é imagem de a pela f) para significar que $(a, b) \in f$. $f : E \longrightarrow F$ será a maneira simbólica de dizermos que f é uma aplicação de E em F. Às vezes, também, usaremos a notação $x \longmapsto f(x)$ para indicarmos a aplicação f em que $f(x)$ é a imagem do elemento genérico x. O conjunto F é chamado *contradomínio* de f.

Notas:

a) Se $f:E \longrightarrow F$ e $g:E \longrightarrow F$ é óbvio (lembrada a definição de relação) que: $f = g \iff f(x) = g(x), \ \forall x \in E$.

b) Se o contradomínio de uma aplicação f é um conjunto numérico (contido em $\mathbb{C}$) é usual chamar-se f de *função*.

Exemplos e contra-exemplos

1º) Se $E = \{0, 1, 2, 3\}$ e $F = \{4, 5, 6, 7, 8\}$, consideremos as relações de E em F seguintes:

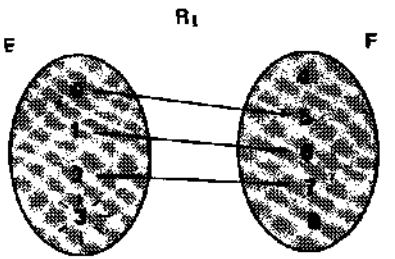
$R_1 = \{(0, 5), (1, 6), (2, 7)\}$

$R_2 = \{(0, 4), (1, 5), (1, 6), (2, 7), (3, 8)\}$

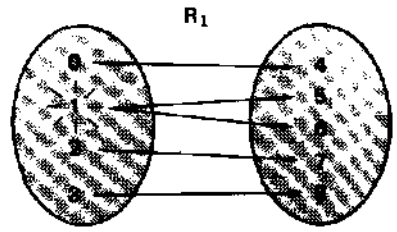
$R_3 = \{(0, 4), (1, 5), (2, 7), (3, 8)\}$

$R_4 = \{(0, 5), (1, 5), (2, 6), (3, 7)\}$

A relação R_1 não é aplicação de E em F pois $D(R_1) = \{0, 1, 2\} \neq E$, isto é, $3 \notin D(R_1)$.



A relação R_2 não é aplicação de E em F pois $(1, 5) \in R_2$ e $(1, 6) \in R_2$, portanto, 1 têm dois "correspondentes" em F.



As relações R_3 e R_4 são aplicações de E em F.

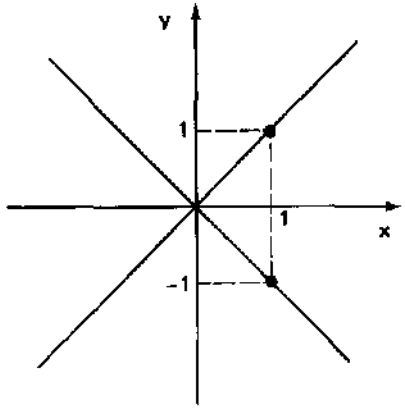
2º) Se $E = F = \mathbb{R}$, consideremos as relações seguintes de $\mathbb{R}$ em $\mathbb{R}$:

$R_1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 = y^2\}$

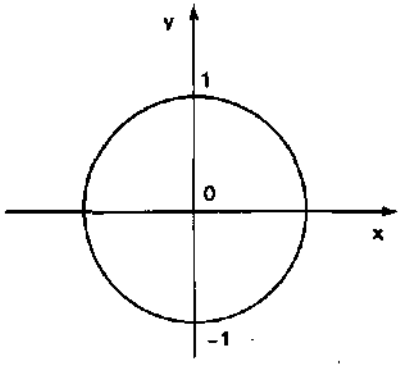
$R_2 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$

$R_3 = \{(x, y) \in \mathbb{R}^2 \mid y = x^2\}$

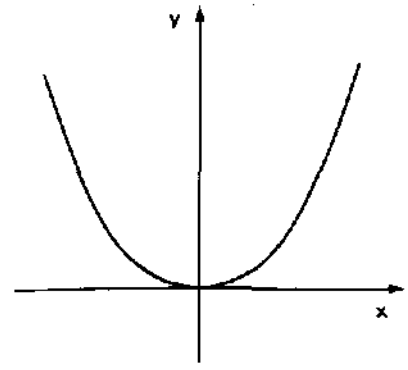
cujos gráficos cartesianos são, respectivamente, assim:



A relação R_1 não é aplicação pois, por exemplo, $x = 1$ se corresponde com $y = 1$ e $y = -1$.



A relação R_2 não é aplicação pois $D(R_2) = [-1, 1] \neq \mathbb{R}$ e também porque $x = 0$, por exemplo, se corresponde com $y = 1$ e $y = -1$.



A relação R_3 é aplicação de $\mathbb{R}$ em $\mathbb{R}$.

2. IMAGEM DIRETA E IMAGEM INVERSA

Seja uma aplicação $f : E \longrightarrow F$.

Definição 23: Dado $A \subset E$, chama-se *imagem direta de A*, segundo f, e indica-se por $f(A)$, o seguinte subconjunto de F:

$$f(A) = \{f(x) \mid x \in A\}$$

isto é, $f(A)$ é o conjunto das imagens por f dos elementos de A.

Definição 24: Dado $B \subset F$, chama-se *imagem inversa de B*, segundo f, e indica-se por $f^{-1}(B)$, o seguinte subconjunto de E:

$$f^{-1}(B) = \{x \in E \mid f(x) \in B\}$$

isto é, $f^{-1}(B)$ é o conjunto dos elementos de E que tem imagem em B através de f.

Exemplos

1º) Se $E = \{1, 3, 5, 7, 9\}$, $F = \{0, 1, 2, 3, \ldots, 10\}$ e $f:E \longrightarrow F$ é dada por $f(x) = x + 1$, temos:

$f(\{3, 5, 7\}) = \{f(3), f(5), f(7)\} = \{4, 6, 8\}$

$f(E) = \{f(1), f(3), f(5), f(7), f(9)\} = \{2, 4, 6, 8, 10\}$

$f(\phi) = \phi$

$f^{-1}(\{2, 4, 10\}) = \{x \in E \mid f(x) \in \{2, 4, 10\}\} = \{1, 3, 9\}$

$f^{-1}(\{0, 1, 3, 5, 7, 9\}) = \{x \in E \mid f(x) \in \{0, 1, 3, 5, 7, 9\}\} = \phi$

2º) Se $E = F = \mathbb{R}$ e $f:\mathbb{R} \longrightarrow \mathbb{R}$ é dada pela lei $f(x) = x^2$, temos:

$f(\{1, 2, 3\}) = \{1, 4, 9\}$

$f([0, 2]) = \{f(x) \mid 0 \leqslant x \leqslant 2\} = \{x^2 \mid 0 \leqslant x \leqslant 2\} = [0, 4]$

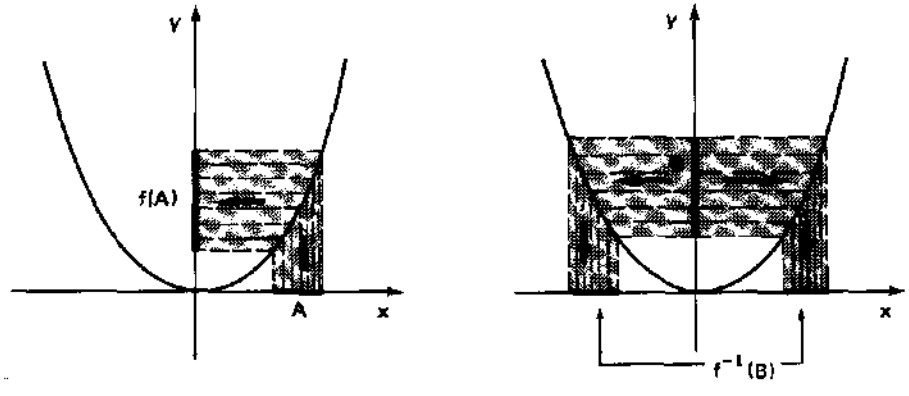
$f(]-1, 3]) = \{x^2 \mid -1 < x \leqslant 3\} = [0, 9]$

$f^{-1}(\{0, 4, 16\}) = \{x \in \mathbb{R} \mid x^2 \in \{0, 4, 16\}\} = \{0, \pm 2, \pm 4\}$

$f^{-1}([1, 9]) = \{x \in \mathbb{R} \mid 1 \leqslant x^2 \leqslant 9\} = [-3, -1] \cup [1, 3]$

$f^{-1}(\mathbb{R}^*) = \{x \in \mathbb{R} \mid x^2 < 0\} = \phi$

Os gráficos abaixo ilustram, respectivamente, como obter f(A) e $f^{-1}(B)$ de maneira gráfica:



3º) Seja $f : \mathbb{R} \longrightarrow \mathbb{R}$ tal que:

$$f(x) = \begin{cases} 0, \text{ se } x \in \mathbb{Q} \\ 1, \text{ se } x \in \mathbb{R} - \mathbb{Q} \end{cases}$$

Temos:

$f(\mathbb{Q}) = \{f(x) \mid x \in \mathbb{Q}\} = \{0\}$

$f(\mathbb{R} - \mathbb{Q}) = \{f(x) \mid x \in \mathbb{R} - \mathbb{Q}\} = \{1\}$

$f([0, 1]) = \{0, 1\}$

$f^{-1}(\{0\}) = \{x \in \mathbb{R} \mid f(x) = 0\} = \mathbb{Q}$

$f^{-1}([4, 5]) = \{x \in \mathbb{R} \mid 4 \leqslant f(x) \leqslant 5\} = \phi$

3. APLICAÇÕES INJETORAS E SOBREJETORAS

Consideremos uma aplicação $f : E \longrightarrow F$.

Definição 25: Dizemos que f é uma *aplicação injetora ou injeção* quando está verificada a seguinte condição:

$(\forall x_1, x_2 \in E)\ (x_1 \neq x_2 \implies f(x_1) \neq f(x_2))$

isto é, quando elementos distintos de E tem imagens distintas em F.

Notemos que a seguinte proposição, equivalente à anterior, é outra forma de *impor que f seja injetora:*

$(\forall x_1, x_2 \in E)\ (f(x_1) = f(x_2) \implies x_1 = x_2)$

Notemos ainda que uma aplicação *não* é injetora quando:

$(\exists x_1, x_2 \in E)\ (x_1 \neq x_2 \text{ e } f(x_1) = f(x_2))$,

isto é, quando existem dois elementos distintos de E que têm imagens iguais.

Definição 26: Dizemos que f é uma *aplicação sobrejetora* ou *sobrejeção* quando está verificada a seguinte condição:

$$\text{Im}(f) = B$$

ou seja, quando:

$(\forall y)\ (y \in F \implies \exists x \in E \mid y = f(x))$

isto é, quando qualquer elemento de F é imagem de algum x de E, segundo f.

Notemos que uma aplicação *não* é sobrejetora quando:

$(\exists y)\ (y \in F \text{ e } \nexists x \in E \mid y = f(x))$

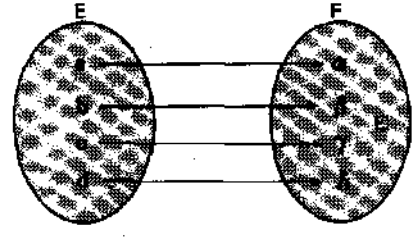
isto é, quando há um elemento de F que não é imagem de elemento algum de E.

Definição 27: Dizemos que f é uma *aplicação bijetora* ou *bijeção* quando f é injetora e sobrejetora.

Exemplos

1º) Se $E = \{a, b, c, d\}$ e $F = \{\alpha, \beta, \gamma, \delta, \varepsilon\}$, a aplicação $f = \{(a, \alpha), (b, \beta), (c, \gamma), (d, \delta)\}$ de E em F é injetora.

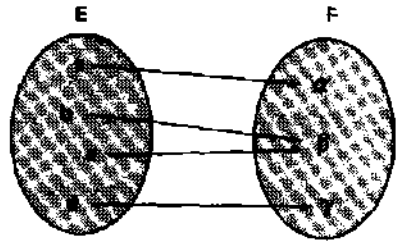
Notemos que no esquema de flechas de uma aplicação injetora não há flechas convergindo para o mesmo ponto de F.



Notemos também que f não é sobrejetora pois $\varepsilon \in F$ e $\varepsilon \notin \text{Im}(f)$.

2º) Se $E = \{a, b, c, d\}$ e $F = \{\alpha, \beta, \gamma\}$, a aplicação $f = \{(a, \alpha), (b, \beta), (c, \beta), (d, \gamma)\}$ de E em F é sobrejetora.

Podemos observar que no esquema de flechas de uma aplicação sobrejetora todo ponto de F é extremidade de alguma flecha.



Vemos também que f não é injetora pois $b \neq c$ e $f(b) = \beta = f(c)$.

3º) A aplicação $f: \mathbb{R} \longrightarrow \mathbb{R}$ *dada pela lei* $f(x) = 3x + 1$ *é bijetora. De fato:*

i) dados $x_1, x_2 \in \mathbb{R}$, temos:
$f(x_1) = f(x_2) \implies 3x_1 + 1 = 3x_2 + 1 \implies x_1 = x_2$
portanto f é injetora;

ii) dado $y \in \mathbb{R}$, provemos que existe $x \in \mathbb{R}$ tal que $f(x) = y$:
$3x + 1 = y \implies x = \frac{y - 1}{3}$
portanto f é sobrejetora.

Nota: As aplicações não podem ser divididas em injetoras ou sobrejetoras porque existem muitas e muitas aplicações que não são nem uma coisa nem outra. Assim, a aplicação $f: \mathbb{R} \longrightarrow \mathbb{R}$ dada pela lei $f(x) = x^2$ não é injetora pois

$$2 \neq -2 \quad \text{e} \quad f(2) = 4 = f(-2)$$

e não é sobrejetora pois

$$-1 \in \mathbb{R} \quad \text{e} \quad -1 \notin \text{Im}(f) = \mathbb{R}_+.$$

4. APLICAÇÃO INVERSA

Seja a aplicação $f: E \longrightarrow F$. Já vimos que f é uma relação de E em F com certas particularidades ($D(f) = E$ e todo $x \in E$ tem imagem única $f(x) \in F$).

Seja f^{-1} *a relação inversa de f. Pode ocorrer que* f^{-1} *não seja uma aplicação de F em E.* Voltando aos exemplos do item anterior, temos:

1º) $f = \{(a, \alpha), (b, \beta), (c, \gamma), (d, \delta)\}$
$f^{-1} = \{(\alpha, a), (\beta, b), (\gamma, c), (\delta, d)\}$
f^{-1} não é aplicação de F em E pois $D(f^{-1}) \neq F$.

2º) $f = \{(a, \alpha), (b, \beta), (c, \beta), (d, \gamma)\}$
$f^{-1} = \{(\alpha, a), (\beta, b), (\beta, c), (\gamma, d)\}$
f^{-1} *não é aplicação de F em E pois* $(\beta, b) \in f^{-1}$ e $(\beta, c) \in f^{-1}$, com $b \neq c$.

O teorema seguinte estabelece a condição para que f^{-1} *seja uma aplicação.*

Teorema 4: *Seja a aplicação* $f: E \longrightarrow F$. Uma condição necessária e suficiente para que f^{-1} seja uma aplicação de F em E é que f seja bijetora.

Demonstração

I. Condição necessária: f^{-1} *é aplicação* $\implies$ *f é bijetora*

a) Sejam $x_1, x_2 \in E$ tais que $f(x_1) = y = f(x_2)$. Então $x_1 = f^{-1}(y)$ e $x_2 = f^{-1}(y)$. Como f^{-1} é aplicação $f^{-1}(y)$ é único, portanto, $x_1 = x_2$. Assim sendo, f é injetora;

b) Seja $y \in F$. Como f^{-1} é aplicação de F em E, existe $x \in E$ tal que $f^{-1}(y) = x$, portanto, $y = f(x)$. Logo f é sobrejetora.

II. Condição suficiente: f é bijetora $\implies$ f^{-1} *é aplicação*

a) Como f é sobrejetora, dado $y \in F$ existe $x \in E$ tal que $y = f(x)$ e, portanto, $(y, x) \in f^{-1}$. Assim, temos que $D(f^{-1}) = F$;

b) Como f é injetora, dados $x_1, x_2 \in E$, temos:

$$f(x_1) = y = f(x_2) \implies x_1 = x_2$$

isto é:

$$(y, x_1) \in f^{-1} \quad \text{e} \quad (y, x_2) \in f^{-1} \implies x_1 = x_2$$

portanto, para todo $y \in F$ é unico o elemento $x \in E$ tal que $(y, x) \in f^{-1}$.

Exemplo

Já vimos que a aplicação $f: \mathbb{R} \longrightarrow \mathbb{R}$ *tal que* $f(x) = 3x + 1$ *é bijetora. Determinemos a aplicação* f^{-1}, inversa de f.

$$f^{-1} = \{(y, x) \in \mathbb{R}^2 \mid (x, y) \in f\} = \{(y, x) \in \mathbb{R}^2 \mid y = 3x + 1\} =$$
$$= \{(x, y) \in \mathbb{R}^2 \mid x = 3y + 1\} = \{(x, y) \in \mathbb{R}^2 \mid y = \frac{x - 1}{3}\}$$

portanto, f^{-1} *é aplicação de* $\mathbb{R}$ *em* $\mathbb{R}$ *dada pela lei* $f^{-1}(x) = \frac{x - 1}{3}$.

Nota: Pode-se provar que se f é bijetora, então f^{-1} também é. Assim, f^{-1} é a aplicação inversa de f e, sendo f^{-1} bijetora, a relação inversa de f^{-1} também é aplicação. Como $(f^{-1})^{-1} = f$, temos que f e f^{-1} são aplicações *inversas entre si.*

5. COMPOSIÇÃO DE APLICAÇÕES

Definição 28: Sejam $f: E \longrightarrow F$ e $g: F \longrightarrow G$. Chama-se *composta de f e g* a aplicação (indicada por gof) de E em G definida da seguinte maneira:

$$(gof)(x) = g(f(x)), \forall x \in E.$$

Exemplos

1º) Sejam $E = \{a_1, a_2, a_3, a_4\}$, $F = \{b_1, b_2, b_3, b_4, b_5\}$ e $G = \{c_1, c_2, c_3\}$. Consideremos as aplicações:

$f = \{(a_1, b_1), (a_2, b_2), (a_3, b_4), (a_4, b_3)\}$ de E em F

$g = \{(b_1, c_1), (b_2, c_1), (b_3, c_2), (b_4, c_2), (b_5, c_3)\}$ de F em G

a aplicação composta de f e g, por definição, é $gof : E \longrightarrow G$ tal que:

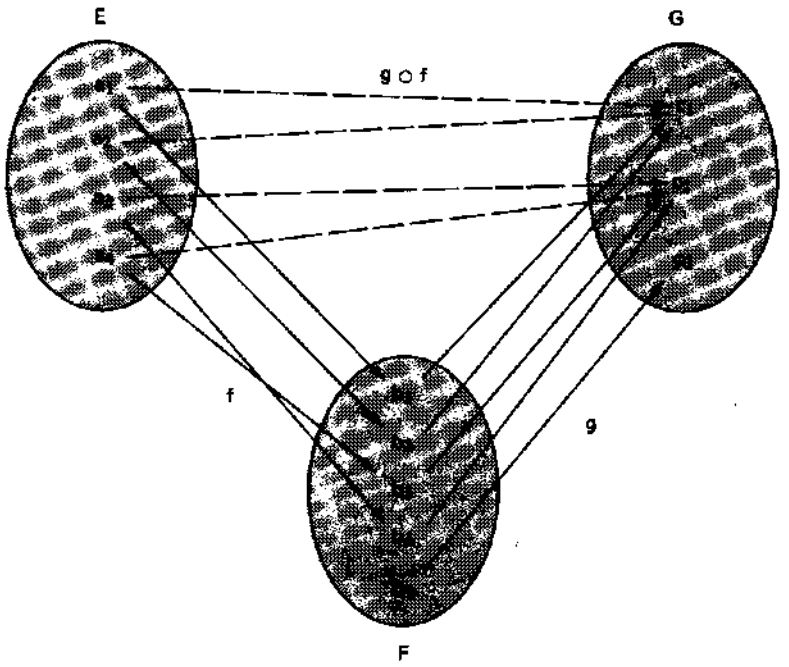
$(gof)(a_1) = g(f(a_1)) = g(b_1) = c_1$

$(gof)(a_2) = g(f(a_2)) = g(b_2) = c_1$

$(gof)(a_3) = g(f(a_3)) = g(b_4) = c_2$

$(gof)(a_4) = g(f(a_4)) = g(b_3) = c_2$

isto é, $gof = \{(a_1, c_1), (a_2, c_1), (a_3, c_2), (a_4, c_2)\}$.



2º) Sejam $f : \mathbb{R} \longrightarrow \mathbb{R}_+$ tal que $f(x) = 2^x$ e $g : \mathbb{R}_+ \longrightarrow \mathbb{R}$ tal que $g(x) = \sqrt{x}$. A aplicação composta de f e g é $gof : \mathbb{R} \longrightarrow \mathbb{R}$ tal que:

$$(gof)(x) = g(f(x)) = \sqrt{f(x)} = \sqrt{2^x}$$

3º) Sendo $f : \mathbb{R} \longrightarrow \mathbb{R}$ tal que $f(x) = 3x$ e $g : \mathbb{R} \longrightarrow \mathbb{R}$ tal que $g(x) = x^2$, a aplicação composta de f e g é $gof : \mathbb{R} \longrightarrow \mathbb{R}$ tal que:

$$(gof)(x) = g(f(x)) = (f(x))^2 = (3x)^2 = 9x^2$$

Notas

(i) A composta de f e g só é definida quando o contra-domínio de f coincide com o domínio de g (conjunto F).

(ii) A composta de f e g tem o mesmo domínio de f (conjunto E) e o mesmo contra-domínio de g(conjunto G).

(iii) Quando E = G, isto é, $f : E \longrightarrow F$ e $g : F \longrightarrow E$ então é possível definir, além de gof, a composta de g e f (indicada por fog) como sendo a aplicação de F em F que obedece à lei $(fog)(x) = f(g(x)), \forall\, x \in F$.

Assim, no 2º exemplo, a composta de g e f é fog: $\mathbb{R}_+ \longrightarrow \mathbb{R}_+$ tal que:

$$(fog)(x) = f(g(x)) = 2^{g(x)} = 2^{\sqrt{x}}$$

No 3º exemplo, a composta de g e f é fog: $\mathbb{R} \longrightarrow \mathbb{R}$ tal que:

$$(fog)(x) = f(g(x)) = 3 \cdot g(x) = 3x^2$$

(iv) Observemos que se $f : E \longrightarrow F$ e $g : F \longrightarrow E$, existem gof e fog, porém, em geral $gof \neq fog$.

Proposição 2: Se $f : E \longrightarrow F$ e $g : F \longrightarrow G$ são injetoras, então gof é injetora.

Demonstração: Sejam $x_1, x_2 \in E$. Temos:

$(gof)(x_1) = (gof)(x_2) \Longrightarrow g(f(x_1)) = g(f(x_2)) \Longrightarrow f(x_1) = f(x_2) \Longrightarrow x_1 = x_2$

Logo gof é injetora. ■

Proposição 3: Se $f : E \longrightarrow F$ e $g : F \longrightarrow G$ são sobrejetoras, então gof é sobrejetora.

Demonstração: Seja $z \in G$. Como g é sobrejetora, existe um $y \in F$ tal que $z = g(y)$. Sendo f sobrejetora, existe um $x \in E$ tal que $y = f(x)$. Assim, temos:

$$z = g(y) = g(f(x)) = (gof)(x)$$

isto prova que gof é sobrejetora. ■

Nota: Quando compomos duas aplicações tais que uma é injetora e a outra sobrejetora, nada podemos afirmar sobre a composta, de maneira geral. No 1º exemplo dado sobre composição de aplicações, f é injetora, g é sobrejetora e gof não é injetora nem sobrejetora.

6. APLICAÇÃO IDÊNTICA

Definição 29: Dado $E \neq \phi$, a aplicação $i_E : E \longrightarrow E$ dada pela lei $i_E(x) = x$ é chamada *aplicação idêntica de E.*

Notemos que para cada E existe uma aplicação idêntica i_E e, ainda, se $E \neq F$ então $i_E \neq i_F$ por terem diferentes domínios.

Proposição 4: Se $f : E \longrightarrow F$ é bijetora, então $f \circ f^{-1} = i_F$ e $f^{-1} \circ f = i_E$.

Demonstração: Já vimos que se f é bijetora, então f^{-1} é uma aplicação bijetora de F em E.

Dado um $x \in F$, temos:

$(f \circ f^{-1})(x) = f(f^{-1}(x)) = x$ portanto $f \circ f^{-1} = i_F$.

Analogamente, dado $x \in E$, temos:

$(f^{-1} \circ f)(x) = f^{-1}(f(x)) = x$ portanto $f^{-1} \circ f = i_E$. ■

Proposição 5: Se $f : E \longrightarrow F$ e $g : F \longrightarrow E$, então:

a) $f \circ i_E = f$, $i_F \circ f = f$, $g \circ i_F = g$ e $i_E \circ g = g$;

b) $g \circ f = i_E$ e $f \circ g = i_F \Longrightarrow$ f e g são bijetoras e $g = f^{-1}$.

Demonstração

a) Provemos, por exemplo, que $f \circ i_E = f$:

$$\left.\begin{array}{l} f : E \longrightarrow F \\ i_E : E \longrightarrow E \end{array}\right\} \Longrightarrow f \circ i_E : E \longrightarrow F \Longrightarrow D(f \circ i_E) = D(f) = E$$

$(f \circ i_E)(x) = f(i_E(x)) = f(x)$, $\forall x \in E$.

b) Provemos, por exemplo, que f é bijetora.

Sendo $x_1, x_2 \in E$, vem:

$f(x_1) = f(x_2) \Longrightarrow g(f(x_1)) = g(f(x_2)) \Longrightarrow i_E(x_1) = i_E(x_2) \Longrightarrow x_1 = x_2$.

e, portanto, f é injetora.

Sendo $y \in F$, vem:

$y = i_F(y) = (f \circ g)(y) = f(g(y)) = f(x)$, onde $x = g(y) \in E$

e, assim, f é sobrejetora.

Analogamente, prova-se que g é bijetora.

Provemos agora que $g = f^{-1}$. Temos:

$D(f^{-1}) = F = D(g)$

$f \circ g = i_F = f \circ f^{-1} \Longrightarrow f(g(x)) = f(f^{-1}(x))$, $\forall x \in F$,

e, como f é injetora, decorre $g(x) = f^{-1}(x)$, $\forall x \in F$. ■

7. RESTRIÇÃO E PROLONGAMENTO

Definição 30: Seja $f : E \longrightarrow F$ e suponhamos $A \subset E$ $(A \neq \phi)$. A aplicação $f \mid A : A \longrightarrow F$ assim definida:

$$(f \mid A)(x) = f(x), \ \forall x \in A$$

é chamada *restrição de f ao subconjunto A.*

Definição 31: Se $B \supset E$ e $C \supset F$ então toda aplicação $g : B \longrightarrow C$ tal que $g(x) = f(x)$, $\forall x \in E$, é chamada *prolongamento de f ao conjunto B.*

Exemplos

1º) Consideremos a função $f : \mathbb{R}^* \longrightarrow \mathbb{R}$ dada por $f(x) = \frac{1}{x}$, $\forall x \in \mathbb{R}^*$.

Se $A = \{2, 4, 6, \ldots\}$, então $f \mid A = \{(2, \frac{1}{2}); (4, \frac{1}{4}), \ldots\}$ é a restrição de f ao conjunto dos números pares maiores que zero.

A função $g : \mathbb{R} \longrightarrow \mathbb{R}$ dada por $g(0) = 0$ e $g(x) = f(x)$, $\forall x \in \mathbb{R}^*$, é um prolongamento de f ao conjunto $\mathbb{R}$.

2º) Seja $f : \mathbb{C} \longrightarrow \mathbb{R}_+$ dada por $f(x + yi) = \sqrt{x^2 + y^2}$.

Seja $\mathbb{R}$ $(\mathbb{R} \subset \mathbb{C})$ e seja $g : \mathbb{R} \longrightarrow \mathbb{R}_+$ dada por $g(x) = |x|$. Neste caso, $g = f \mid \mathbb{R}$ pois:

$f(x) = f(x + 0i) = \sqrt{x^2 + 0^2} = |x| = g(x)$, $\forall x \in \mathbb{R}$.

8. APLICAÇÕES MONÓTONAS

Definição 32: Seja $f : E \longrightarrow F$ e suponhamos E e F parcialmente ordenados.

Dizemos que f é uma aplicação *crescente* em E se

$$(\forall x, x' \in E)\ (x \preccurlyeq x' \Longrightarrow f(x) \preccurlyeq f(x')).$$

Dizemos que f é uma aplicação *decrescente* em E se

$$(\forall x, x' \in E)\ (x \preccurlyeq x' \Longrightarrow f(x') \preccurlyeq f(x)).$$

Uma aplicação crescente ou decrescente será chamada *aplicação monótona.*

Definição 33: Uma *aplicação estritamente monótona em E* é uma aplicação $f : E \longrightarrow F$ que satisfaça a uma das seguintes propriedades:

a) *Estritamente crescente*, isto é,

$$(\forall x, x' \in E)\ (x \prec x' \Longrightarrow f(x) \prec f(x')).$$

b) *Estritamente decrescente* que quer dizer

$(\forall x, x' \in E)\ (x \prec x' \iff f(x') \prec f(x))$.

9. FAMÍLIAS

Há certas oportunidades em que, dada uma aplicação $x : I \longrightarrow F$, o aspecto desta sobre o qual mais se quer chamar a atenção é o conjunto imagem.

Neste caso é usual mudar-se a notação: ao invés de x(i), para indicar a imagem de um elemento $i \in I$, escreve-se x_i. A aplicação é indicada, então, por $(x_i)_{i \in I}$ e recebe o nome de *família*. O conjunto I se denomina *conjunto de índices* da família.

Exemplos:

1) Se $I = \{1, 2, 3, \ldots\}$ então uma família cujo conjunto de índices é I é chamada *seqüência*. $(x_1, x_2, \ldots, x_n, \ldots)$ é como se indica uma seqüencia.

2) Se $I = \{1, 2, \ldots, n\}$, $n \geqslant 1$, chamaremos de *seqüência finita* ou *n-upla* uma família cujo conjunto de índices é I. Sua notação é, pois, $(x_1, x_2, \ldots, x_n)$.

EXERCÍCIOS

52. Sendo $E = \{a, b, c, d\}$ e $F = \{1, 2, 3\}$, decida quais das relações abaixo são aplicações de E em F.

$R_1 = \{(a, 1), (b, 2), (c, 3)\}$

$R_2 = \{(a, 1), (b, 1), (c, 2), (d, 3)\}$

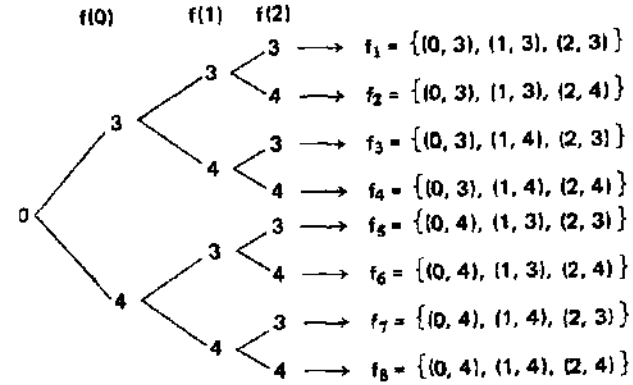
$R_3 = \{(a, 1), (a, 2), (b, 1), (c, 2), (d, 3)\}$

$R_4 = \{(a, 2), (b, 2), (c, 2), (d, 2)\}$

53. Determinar todas as aplicações de $E = \{0, 1, 2\}$ em $F = \{3, 4\}$.

Solução

A cada elemento de E associemos como imagem um (e um só) elemento de F.
Para imagem de 0 podemos escolher 3 ou 4.
Escolhida a imagem de 0, para imagem de 1 podemos tomar 3 ou 4 (a imagem de 1 *independe da de 0*).
Escolhidas as imagens de 0 e de 1, para imagem de 2 podemos tomar também 3 ou 4.
Temos, então, 8 possíveis aplicações de E em F, como mostra o diagrama abaixo, chamado árvore de possibilidades:



54. *Se E e F são conjuntos finitos com m e n elementos, respectivamente, quantas são as aplicações de E em F?*

55. Escrever como conjunto de pares ordenados a função $f:E \longrightarrow F$ tal que $f(x) = 1$, se $x \in Q$, e $f(x) = -1$, se $x \notin Q$. São dados $E = \{0, 1, \frac{1}{2}, \sqrt{2}, \pi, \frac{7}{3}\}$ e $F = \{-1, 1\}$.

56. Seja a aplicação $f: \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ tal que $f(x, y) = mdc(x, y)$. Determinar f(5, 1), f(12, 8), f(3, 7), f(0, 5) e f(0, 0).

57. A aplicação $f: \mathbb{R} \longrightarrow \mathbb{R}$ é tal que

$$f(x) = \begin{cases} 2x + 5, & \text{quando } x < -1 \\ x^2 - 1, & \text{quando } -1 \leqslant x \leqslant 1 \\ 5x, & \text{quando } x > 1 \end{cases}$$

Determinar $f(0)$, $f(\frac{5}{3})$, $f(-\frac{7}{2})$, $f(\sqrt{2})$, e $f(-\frac{2\pi}{5})$.

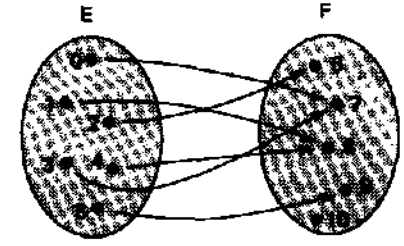
58. Decidir em cada caso se f e g são funções iguais.

1º) $f(x) = \dfrac{x^2 - 4x + 3}{x - 3}$, $g(x) = x - 1$ e $x \in \mathbb{R} - \{3\}$

2º) $f(x) = 1$, $g(x) = x^4$ e $x \in \{1, -1, i, -i\}$

3º) $f(x) = x^3$, $x \in \mathbb{R}$ e $g(y) = y^3$, $y \in [-1, 1]$

59. Ao lado está o diagrama representativo de uma função $f : E \longrightarrow F$. Determinar $f(\{0, 1\})$, $f(\{3, 4\})$, $f(\{1, 2, 5\})$, $f(E)$, $f^{-1}(\{7, 8\})$ e $f^{-1}(\{9, 10\})$.



60. Seja a função $f:\mathbb{R} \longrightarrow \mathbb{R}$ dada por $f(x) = |x|$.
Determinar $f(1)$, $f(-3)$, $f(1-\sqrt{2})$, $f([-1, 1])$, $f(]-1, 2])$, $f(\mathbb{R})$, $f^{-1}([0, 3])$, $f^{-1}([-1, 3$ e $f^{-1}(\mathbb{R}_-^*)$.

61. Seja a função $f: \mathbb{R} \longrightarrow \mathbb{R}$ dada pela seguinte lei:

$$f(x) = \begin{cases} x^2, & \text{se } x \leqslant 0 \\ \sqrt[3]{x}, & \text{se } x > 0 \end{cases}$$

Determinar $f([-1, 8])$, $f(\mathbb{R}_-)$, $f(\mathbb{R}_+)$, $f^{-1}(\{1, 16\})$, $f^{-1}([-1, 16])$ e $f^{-1}(\mathbb{R}^*)$.

62. Seja a função $f: \mathbb{R} \longrightarrow \mathbb{R}$ dada por $f(x) = \cos x$.
Determinar $f([0, \frac{\pi}{2}])$, $f([0, \pi])$, $f(\mathbb{R})$, $f^{-1}(\{\frac{1}{2}\})$, $f^{-1}([\frac{1}{2}, 1])$ e $f^{-1}(\mathbb{R}_-)$.

63. Seja $f: E \longrightarrow F$ uma aplicação e sejam $A \subset E$ e $B \subset E$. Provar que:
a) se $A \subset B$ então $f(A) \subset f(B)$
b) $f(A \cup B) = f(A) \cup f(B)$
c) $f(A \cap B) \subset f(A) \cap f(B)$
d) $A \subset f^{-1}(f(A))$ e $f(f^{-1}(B)) \subset B$
e) f é bijetora se, e somente se, $f(A^C) = (f(A))^C$, $\forall A \subset E$ *

64. Abaixo estão indicadas algumas aplicações de $E = \{a, b, c, d\}$ em $F = \{0, 1, 2, 3, 4\}$. Quais são injetoras?
$f_1 = \{(a, 0), (b, 1), (c, 2), (d, 4)\}$
$f_2 = \{(a, 1), (b, 2), (c, 3), (d, 1)\}$
$f_3 = \{(a, 2), (b, 4), (c, 3), (d, 0)\}$
$f_4 = \{(a, 3), (b, 0), (c, 0), (d, 4)\}$

65. Quais das seguintes aplicações de $E = \{a, b, c\}$ em $F = \{0, 1\}$ são sobrejetoras?
$f_1 = \{(a, 0), (b, 0), (c, 0)\}$
$f_2 = \{(a, 0), (b, 0), (c, 1)\}$
$f_3 = \{(a, 1), (b, 0), (c, 1)\}$
$f_4 = \{(a, 1), (b, 1), (c, 1)\}$

66. Determinar todas as injeções de $A = \{1, 2\}$ em $B = \{3, 4, 5\}$.

67. Determinar todas as sobrejeções de $A = \{1, 2, 3\}$ em $B = \{4, 5\}$.

68. Se E e F são conjuntos finitos com m e n elementos, respectivamente, quantas são as aplicações injetoras de E em F? E quantas são as sobrejetoras?

69. Mostrar que toda aplicação injetora (sobrejetora) de um conjunto finito em si mesmo é também sobrejetora (injetora).

* Se $L \subset Y$, L^C é o complementar de L em relação a Y.

70. Classificar (se possível) em injetora ou sobrejetora as seguintes funções de $\mathbb{R}$ em $\mathbb{R}$.
a) $y = x^3$
b) $y = x^2 - 5x - 6$
c) $y = 2^x$
d) $y = |\text{sen } x|$
e) $y = x + |x|$
f) $y = x + 3$
g) $y = \text{tg } x$, $x \neq \frac{\pi}{2} + k\pi$ $(k \in \mathbb{Z})$
$y = 0$, $x = \frac{\pi}{2} + k\pi$ $(k \in \mathbb{Z})$

71. Achar uma função $f: A \longrightarrow B$, com A e B subconjuntos de $\mathbb{R}$, para cada caso abaixo:
a) $A = \mathbb{R}$, $B \subsetneq \mathbb{R}$ e f injetora e não sobrejetora
b) $A \subsetneq \mathbb{R}$, $B = \mathbb{R}$ e f injetora e não sobrejetora
c) $A = \mathbb{R}$, $B \subsetneq \mathbb{R}$ e f sobrejetora e não injetora
d) $A \subsetneq \mathbb{R}$, $B = \mathbb{R}$ e f sobrejetora e não injetora

72. Mostrar que $f: \mathbb{R} \longrightarrow \mathbb{R}$ definida por $f(x) = ax + b$, com a e b constantes reais, $a \neq 0$, é uma bijeção. Obter f^{-1}.

73. Mostrar que $f: \mathbb{R} - \{-\frac{d}{c}\} \longrightarrow \mathbb{R} - \{\frac{a}{c}\}$ dada pela sentença $y = \frac{ax + b}{cx + d}$, onde a, b, c, d são constantes reais, $ad - bc \neq 0$, é uma bijeção. Descrever a aplicação f^{-1}.

74. Provar que a função $f:]-1, 1[\longrightarrow \mathbb{R}$ definida pela lei $f(x) = \frac{x}{1 - |x|}$ é bijetora.
Definir sua inversa.

75. Seja $f: \mathbb{R}^2 \longrightarrow \mathbb{R}$ dada por $f(x, y) = xy$.
a) f é injetora?
b) f é sobrejetora?
c) obter $f^{-1}(\{0\})$
d) obter $f([0, 1] \times [0, 1])$
e) obter $f(\Delta_R)$ onde $\Delta_R = \{(x, y) \mid x = y\}$

76. Considere a aplicação $f: \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ tal que $f(x, y) = (2x + 3, 4y + 5)$. Prove que f é injetora. Verifique se f é bijetora.

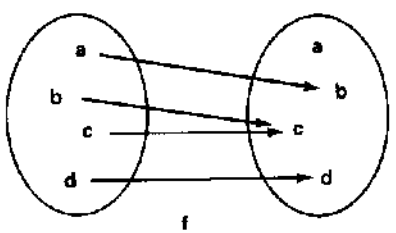
77. Mostrar, em cada caso, que os conjuntos A e B são *equipotentes* (*).
1º) $A = \mathbb{N}$ e $B = \mathbb{N}^*$
2º) $A = \mathbb{Z}$ e $B = \mathbb{N}$
3º) $A = \mathbb{R}$ e $B = \mathbb{R}_+^*$
4º) $A =]-\frac{\pi}{2}, \frac{\pi}{2}[$ e $B = \mathbb{R}$
5º) $A =]-1, 1[$ e $B =]a, b[$, com $a < b$, a e b reais
6º) $A =]-1, 1[$ e $B = [-1, 1]$
7º) $A =]-1, 1[$ e $B = \mathbb{R}$
Sugestão: descubra, em cada caso, $f: A \longrightarrow B$ bijetora.

(*) Dois conjuntos A e B são equipotentes quando $A = B = \phi$ ou existe $f: A \longrightarrow B$ bijetora.

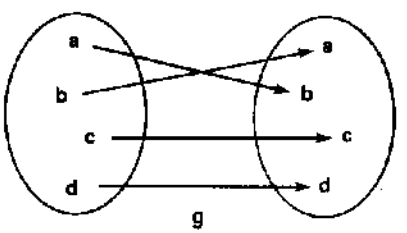
78. Provar que se uma função f é inversível e seu gráfico é uma curva simétrica em relação à reta $y = x$, então $f = f^{-1}$. Dar exemplos de funções f tais que $f = f^{-1}$.

79. Sejam $A = \{1, 2, 3\}$, $B = \{4, 5, 6, 7\}$ e $C = \{8, 9, 0\}$.
Seja $f: A \longrightarrow B$ dada por $f(1) = 4$, $f(2) = 5$, $f(3) = 6$.
Seja $g: B \longrightarrow C$ dada por $g(4) = 8$, $g(5) = 8$, $g(6) = 9$ e $g(7) = 0$.
Quais são os pares ordenados de $g \circ f$. A função $g \circ f$ é injetora ou sobrejetora?

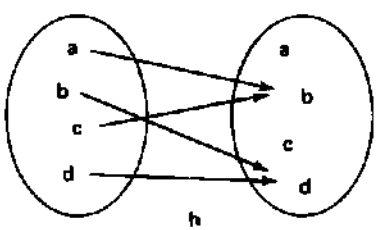
80. Sejam as funções f, g e h dadas pelos diagramas abaixo.
Determinar as funções compostas $g \circ f$, $f \circ g$, $g \circ h$, $h \circ f$ e $h \circ h$.



f



g



h

81. Sejam f, g, h funções reais definidas por $f(x) = x - 1$, $g(x) = x^2 + 2$ e $h(x) = x + 1$.
a) Determinar $f \circ g$; $f \circ h$; $g \circ h$; $g \circ f$; $h \circ f$; $h \circ g$;
b) Verificar que $(f \circ g) \circ h = f \circ (g \circ h)$.

82. Dadas as funções $f = \{(x, y) \in \mathbb{R}^2 \mid y = x^3 + 1\}$ e $g = \{(x, y) \in \mathbb{R}^2 \mid y = x^2 + 1\}$, determinar as compostas $f \circ g$, $g \circ f$, $f \circ f$ e $g \circ g$.

83. Sejam as funções reais $f(x) = \operatorname{sen} x$ e $g(x) = |x|$. Esboçar os gráficos das compostas $f \circ g$ e $g \circ f$.

84. Sejam $f: \mathbb{R} \longrightarrow \mathbb{R}$ e $g: \mathbb{R} \longrightarrow \mathbb{R}$ as aplicações assim definidas:

$$f(x) = \begin{cases} x + 1, \text{ se } x \geqslant 0 \\ -x + 1, \text{ se } x < 0 \end{cases} \quad \text{e} \quad g(x) = 3x - 2$$

Determinar as compostas $f \circ g$ e $g \circ f$.

Solução

1ª parte : $f \circ g$

a) Se $3x - 2 \geqslant 0$, temos:

$(f \circ g)(x) = f(g(x)) = g(x) + 1 = (3x - 2) + 1 = 3x - 1$

b) Se $3x - 2 < 0$, temos:

$(f \circ g)(x) = f(g(x)) = -g(x) + 1 = -(3x - 2) + 1 = -3x + 3$

portanto:

$$(f \circ g)(x) = \begin{cases} 3x - 1, \text{ se } x \geqslant 2/3 \\ -3x + 3, \text{ se } x < 2/3 \end{cases}$$

2ª Parte : $g \circ f$

a) Se $x \geqslant 0$, temos:

$(g \circ f)(x) = g(f(x)) = 3f(x) - 2 = 3(x + 1) - 2 = 3x + 1$

b) Se $x < 0$, temos:

$(g \circ f)(x) = g(f(x)) = 3f(x) - 2 = 3(-x + 1) - 2 = -3x + 1$

portanto:

$$(g \circ f)(x) = \begin{cases} 3x + 1, \text{ se } x \geqslant 0 \\ -3x + 1, \text{ se } x < 0 \end{cases}$$

85. Determinar as compostas $f \circ g$ e $g \circ f$ sabendo que f e g são funções de $\mathbb{R}$ em $\mathbb{R}$ tais que:

$$f(x) = \begin{cases} x^2, \text{ se } x < 0 \\ 2x, \text{ se } x \geqslant 0 \end{cases} \quad \text{e} \quad g(x) = \begin{cases} 1 - x, \text{ se } x < 1 \\ 1 + x, \text{ se } x \geqslant 1 \end{cases}$$

86. Determinar as compostas $g \circ f$ e $f \circ g$ das seguintes funções de $\mathbb{R}$ em $\mathbb{R}$:

$$f(x) = \begin{cases} x^2 + 1, \text{ se } x < 0 \\ 2x + 1, \text{ se } x \geqslant 0 \end{cases} \quad \text{e} \quad g(x) = \begin{cases} 3x, \text{ se } x < 1 \\ 7x + 1, \text{ se } 1 \leqslant x \leqslant 5 \\ 2 + x, \text{ se } x > 5 \end{cases}$$

87. Sendo $f: \mathbb{R} \longrightarrow \mathbb{R}$ uma função dada pela lei $f(x) = x + 1$, para $x \leqslant 0$, e $f(x) = 1 - 2x$, para $x > 0$, determinar $f \circ f$.

88. Sendo $f(x) = ax^n$, $n \in \mathbb{N}^*$, determinar a e n de modo que $(f \circ f)(x) = 3x^4$.

89. Sejam as funções reais $f(x) = 2x + 7$ e $(f \circ g)(x) = 4x^2 - 2x + 3$. Determinar a lei da função g.

90. Determinar $f \circ g$ e $g \circ f$, quando $f: \mathbb{R}^* \longrightarrow \mathbb{R} - \{1\}$ é tal que $f(x) = \dfrac{x + 2}{x}$ e $g: \mathbb{R} - \{1\} \longrightarrow \mathbb{R}^*$ é tal que $g(x) = \dfrac{2}{x - 1}$. Que se conclui daí?

91. a) *Sendo* $f: \mathbb{N} \longrightarrow \mathbb{N}$ *tal que* $f(n) = n+1$, *mostrar que há infinitas funções* $g: \mathbb{N} \longrightarrow \mathbb{N}$ tal que $g \circ f = i_{\mathbb{N}}$. A função f é inversível?

b) Sendo $g : \mathbb{N} \to \mathbb{N}$ tal que $g(n) = \frac{n}{2}$ se n é par e $g(n) = \frac{n+1}{2}$ se n é ímpar, mostre que existem infinitas funções $h : \mathbb{N} \to \mathbb{N}$ tais que $g \circ h = i_{\mathbb{N}}$. A função g é inversível?

92. *Se* $f: E \longrightarrow F$ *e* $g: F \longrightarrow E$ *são tais que* $g \circ f = i_E$, quais das seguintes conclusões são válidas?

a) $g = f^{-1}$;
b) f é sobrejetora;
c) f é injetora;
d) g é injetora;
e) g é sobrejetora.

93 Sejam as aplicações $f: E \longrightarrow F$ e $g: F \longrightarrow E$. Provar que:

a) *se* $g \circ f$ *é injetora, então f é injetora;*

b) se $f \circ g$ é sobrejetora, então f é sobrejetora.

94. Sejam $f: E \longrightarrow F$; $g: E \longrightarrow F$; $h: F \longrightarrow G$. Supondo h injetora e $h \circ g = h \circ f$, provar que $g = f$.

95. Sejam $f: E \longrightarrow F$ e $g: F \longrightarrow G$. Supondo g bijetora, provar que f é injetora se, e *somente se*, $g \circ f$ também é injetora.

96. Quais das funções abaixo são restrições da função $f: \mathbb{R} \longrightarrow \mathbb{R}$ tal que $f(x) = x^2$?

a) $g = \{(0, 0), (1, 1), (2, 4)\}$ de $\{0, 1, 2\}$ em $\{0, 1, 4\}$
b) $h(x) = x^2$ de $\mathbb{C}$ em $\mathbb{C}$
c) $i_{\{0, 1\}}$ = aplicação idêntica de $\{0, 1\}$.

97. Quais das funções abaixo são prolongamentos de $i_{\mathbb{Z}}$?

a) $f: \mathbb{R} \longrightarrow \mathbb{Z}$ tal que $f(x) = [x]$ = maior inteiro contido em x.
b) $i_{\mathbb{R}}$
c) $g: \mathbb{R} \longrightarrow \mathbb{R}$ tal que $g(x) = [x]$

98. Considere a seguinte família de subconjuntos de $\mathbb{R}$: $\mathcal{F} = (A_i)_{i \in \mathbb{N}^*}$ onde $A_i = [0, 1 + \frac{1}{i}[$. Acha a "união" $\bigcup_{i \in \mathbb{N}^*} A_i$ e a "intersecção" $\bigcap_{i \in \mathbb{N}^*} A_i$.

99. Considere a família de retas $(A_k)_{k \in \mathbb{R}}$ onde $A_k = \{(x, y) \in \mathbb{R}^2 \mid y = x + k\}$. O que é $\bigcup_{k \in \mathbb{R}} A_k$ E $\bigcap_{k \in \mathbb{R}} A_k$?

100. Considere a família de conjuntos A_k onde $A_k = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = k^2, k \geq 1\}$. Descrever os conjuntos $\bigcup A_k$ e $\bigcap A_k$.

§ 5º — OPERAÇÕES — LEIS DE COMPOSIÇÃO INTERNAS

1. EXEMPLOS PRELIMINARES

a) Consideremos a aplicação $f: \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ tal que $f(x, y) = x + y$. Dados dois números *x* e *y* naturais, ao par (x, y) a aplicação f associa sua soma x + y. A aplicação f é conhecida como *operação de adição sobre* $\mathbb{N}$.

b) Seja a aplicação $f: \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ tal que $f(x, y) = x \cdot y$, isto é, f associa a cada par (x, y) de números reais o seu produto x . y. Esta aplicação é conhecida com o nome de *operação de multiplicação sobre* $\mathbb{R}$.

c) Sendo $\mathcal{F}$ uma coleção de conjuntos, consideremos a aplicação $f: \mathcal{F} \times \mathcal{F} \longrightarrow \mathcal{F}$ tal que $f(X, Y) = X \cap Y$, isto é, a aplicação que associa ao par de conjuntos (X, Y) a sua intersecção $X \cap Y$. Esta aplicação é conhecida com o nome de *operação de intersecção sobre* $\mathcal{F}$.

2. CONCEITUAÇÃO

Definição 34: Sendo E um conjunto não vazio, toda aplicação $f: E \times E \longrightarrow E$ *recebe o nome de operação sobre E ou lei de composição interna em E.*

Nas considerações de caráter geral que faremos a seguir neste parágrafo, uma *operação f sobre E associa a cada par (x, y) de ExE um elemento x∗y (lê-se: "x estrela y") de E, isto é, x∗y é uma outra forma de indicar f(x, y). Diremos também que E é um conjunto munido da operação* ∗ .

O elemento x∗y chama-se *composto de x e y* pela operação f; os elementos *x* e *y* do composto x∗y são chamados *termos* do composto x∗y; os termos *x* e *y* do composto x∗y são chamados, respectivamente, primeiro e segundo termos ou, então, termo da esquerda e termo da direita.

Outras *notações poderão ser* usadas para indicar uma operação sobre E:

a) *notação aditiva*

Neste caso, o símbolo da operação é +, a operação é chamada *adição*, o composto x + y é chamado *soma* e os termos *x* e *y* são as *parcelas*.

b) *notação multiplicativa*

Neste caso, o símbolo da operação é ., a operação é chamada *multiplicação*, o composto x . y é chamado *produto* e os termos *x* e *y* são os fatores.

c) *notação de composição*

Neste caso, o símbolo da operação é $\circ$ e a operação é denominada *composição.*

d) outros símbolos utilizados para operações genéricas são Δ(triângulo), x, T, $\perp$, $\otimes$, $\oplus$, etc.

3. OUTROS EXEMPLOS

1º) A aplicação f: $\mathbb{N}\times\mathbb{N} \longrightarrow \mathbb{N}$ tal que $f(x, y) = x^y$ é a operação de potenciação sobre $\mathbb{N}$.

Observemos que, quaisquer que sejam os naturais x e y, o símbolo x^y representa um número natural, portanto, f está bem definida. Observemos ainda que esta operação não pode ser estendida a $\mathbb{Z}$ porque, por exemplo, a imagem de (2, -1) seria $2^{-1} \notin \mathbb{Z}$. Também não pode ser estendida a $\mathbb{Q}$ (porque, por exemplo, $(2, \frac{1}{2}) \in \mathbb{Q}\times\mathbb{Q}$ e $2^{1/2} \notin \mathbb{Q}$) e nem a $\mathbb{R}$ (porque, por exemplo, $(-1, \frac{1}{2}) \in \mathbb{R}\times\mathbb{R}$ e $(-1)^{1/2} \notin \mathbb{R}$)

2º) A aplicação f: $\mathbb{Q}\times\mathbb{Q}^* \longrightarrow \mathbb{Q}^*$ tal que $f(x, y) = \frac{x}{y}$ é a operação de divisão sobre $\mathbb{Q}$.

Fica como exercício arranjar exemplos que mostrem que não se pode definir uma operação de divisão em $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$.

A operação de divisão pode ser definida também em $\mathbb{R}^*$ e $\mathbb{C}^*$.

3º) A aplicação f: $\mathbb{Z}\times\mathbb{Z} \longrightarrow \mathbb{Z}$ tal que $f(x, y) = x - y$ é a operação de subtração sobre $\mathbb{Z}$. A subtração pode ser estendida a $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$.

4º) A aplicação f: $E \times E \longrightarrow E$, onde $E = M_{m\times n}(\mathbb{R})$ = conjunto das matrizes do tipo mxn com elementos reais, tal que $f(x, y) = x + y$ é a operação de adição sobre $M_{m\times n}(\mathbb{R})$.

5º) A aplicação f: $E \times E \longrightarrow E$, onde $E = M_n(\mathbb{R})$, tal que $f(x, y) = x \cdot y$ é a operação de multiplicação sobre $M_n(\mathbb{R})$. (*)

6º) A aplicação φ: $E \times E \longrightarrow E$, onde $E = \mathbb{R}^{\mathbb{R}}$ = conjunto das funções de $\mathbb{R}$ em $\mathbb{R}$, tal que $\varphi(f, g) = f \circ g$ é a operação de composição sobre $\mathbb{R}^{\mathbb{R}}$.

(*) $M_n(\mathbb{R})$ indica o conjunto das matrizes reais n por n.

4. PROPRIEDADES DAS OPERAÇÕES

Seja $*$ uma lei de composição interna em E. Vejamos algumas propriedades notáveis que $*$ pode apresentar.

a) Propriedade associativa

Definição 35: Dizemos que $*$ tem a propriedade associativa quando

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

quaisquer que sejam $x, y, z \in E$.

Exemplos

1º) As adições em $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ são operações associativas, isto é, operações que gozam da propriedade associativa.

2º) As multiplicações em $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ são operações associativas.

3º) A adição em $M_{m\times n}(\mathbb{R})$ conjunto das matrizes do tipo mxn com elementos reais, é operação associativa.

4º) A multiplicação em $M_n(\mathbb{R})$ é associativa.

5º) A composição de funções de $\mathbb{R}$ em $\mathbb{R}$ é associativa.

Contra-exemplos

1º) A potenciação em $\mathbb{N}$ não é associativa pois:

$2^{(3^4)} = 2^{81}$ e $(2^3)^4 = 2^{12}$

2º) A divisão em $\mathbb{R}^*$ não é associativa pois:

$(24 : 4) : 2 = 6 : 2 = 3$ e $24 : (4 : 2) = 24 : 2 = 12$

Observação: O fato de uma operação ser associativa permite que calculemos o composto de mais de dois elementos sem necessidade de usar os parênteses, uma vez que qualquer associação entre os elementos conduz ao mesmo resultado final. Por exemplo:

$2 + 3 + 5 + 8 = (2 + 3) + (5 + 8) = 2 + (3 + 5) + 8 = 2 + (3 + 5 + 8) = 18$

Se uma operação não é associativa, temos obrigação de usar parênteses para indicar como deve ser calculado um composto de três ou mais elementos, caso contrário deixamos o composto sem significado. Por exemplo:

$48 : 4 : 2 : 6$ não tem significado

$(48 : 4) : (2 : 6) = 12 : \frac{1}{3} = 36$

$48 : (4 : 2) : 6 = 48 : 2 : 6$ não tem significado

$48 : ((4 : 2) : 6) = 48 : (2 : 6) = 48 : \frac{1}{3} = 144$

b) Propriedade comutativa

Definição 36: Dizemos que $*$ tem a propriedade comutativa quando

$$x*y = y*x$$

quaisquer que sejam $x, y \in E$.

Exemplos

1º) As adições em $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são operações comutativas.

2º) As multiplicações em $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são operações comutativas.

3º) A adição em $M_{m\times n}(\mathbb{R})$ é comutativa

Contra-exemplos

1º) A potenciação em $\mathbb{N}$ não é comutativa pois:
$2^3 = 8$ e $3^2 = 9$.

2º) A divisão em $\mathbb{R}^*$ não é comutativa pois:
$1 : 5 = \frac{1}{5}$ e $5 : 1 = 5$.

3º) A subtração em $\mathbb{Z}$ não é comutativa pois:
$2 - 4 = -2$ e $4 - 2 = 2$.

4º) A multiplicação em $M_{2x2}(\mathbb{R})$ não é comutativa pois:

$$\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}.\begin{pmatrix}4 & 5\\ 6 & 7\end{pmatrix} = \begin{pmatrix}16 & 19\\ 36 & 43\end{pmatrix} \text{ e}$$

$$\begin{pmatrix}4 & 5\\ 6 & 7\end{pmatrix}.\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix} = \begin{pmatrix}19 & 28\\ 27 & 40\end{pmatrix}$$

5º) A composição em $\mathbb{R}^{\mathbb{R}}$ (conjunto das funções de $\mathbb{R}$ em $\mathbb{R}$) não é comutativa pois, se $f(x) = 2x$ e $g(x) = x^2$, então:
$(f \circ g)(x) = f(g(x)) = 2x^2$ e
$(g \circ f)(x) = g(f(x)) = (2x)^2 = 4x^2$

c) Elemento neutro

Definição 37: Dizemos que $e \in E$ é um *elemento neutro à esquerda* para a operação $*$ quando:

$$e * x = x$$

para todo $x \in E$.

Dizemos que $e \in E$ é um *elemento neutro à direita* para a operação $*$ quando:

$$x * e = x$$

para qualquer $x \in E$.

Se e é elemento neutro à direita e à esquerda para $*$, então dizemos que e é *elemento neutro* para esta lei.

Exemplos:

1º) O elemento neutro das adições em $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ é o número 0 pois $0 + x = x = x + 0$ para qualquer número x.

2º) O elemento neutro das multiplicações em $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ é o número 1 pois $1 \cdot x = x = x \cdot 1$ para qualquer número x.

3º) O elemento neutro da adição em $M_{m \times n}(\mathbb{R})$ é a matriz nula do tipo m x n pois:

$$0_{m\times n} + X = X = X + 0_{m\times n}$$

qualquer que seja $X \in M_{m\times n}(\mathbb{R})$. (Obs.: $0_{m\times n} = \begin{pmatrix}0 & 0 & \dots & 0\\ 0 & 0 & \dots & 0\\ \dots & \dots & \dots & \dots\\ 0 & 0 & \dots & 0\end{pmatrix}$).

4º) $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ é o elemento neutro da multiplicação em $M_{2\times 2}(\mathbb{R})$ pois:

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix} = \begin{pmatrix}a & b\\ c & d\end{pmatrix} = \begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

quaisquer que sejam $a, b, c, d \in \mathbb{R}$.

5º) O elemento neutro da composição em $\mathbb{R}^{\mathbb{R}}$ é a função $i_{\mathbb{R}}$ (idêntica em $\mathbb{R}$) pois:

$$i_{\mathbb{R}} \circ f = f = f \circ i_{\mathbb{R}}$$

qualquer que seja $f \in \mathbb{R}^{\mathbb{R}}$.

Contra-exemplos

1º) A subtração em $\mathbb{Z}$ admite 0 como elemento neutro à direita pois $x - 0 = x, \forall x \in \mathbb{Z}$ mas não tem neutro à esquerda pois não existe e (fixo) tal que $e - x = x, \forall x \in \mathbb{Z}$.

2º) A divisão em $\mathbb{R}^*$ admite 1 como elemento neutro à direita pois $x : 1 = x, \forall x \in \mathbb{R}^*$ mas não tem neutro à esquerda pois não existe e (fixo) tal que $e : x = x, \forall x \in \mathbb{R}^*$.

3º) A operação $*$ tal que $x * y = y$ sobre $\mathbb{R}$ tem infinitos elementos neutros à esquerda pois $e * y = y, \forall y \in \mathbb{R}$ é satisfeita por qualquer $e \in \mathbb{R}$, mas não tem neutro à direita pois não existe e (fixo) tal que $x * e = x, \forall x \in \mathbb{R}$.

Proposição 6: Se a operação $*$ tem um elemento neutro e, ele é único.

Demonstração: Sejam e e e' elementos neutros da operação $*$.

Temos:

e neutro $\Longrightarrow$ $e * e' = e'$

e' neutro $\Longrightarrow$ $e * e' = e$

então $e = e'$. ■

d) Elementos simetrizáveis

Definição 38: Dizemos que $x \in E$ é um elemento simetrizável, para a operação $*$ que tem neutro *e*, se existe $x' \in E$ tal que:

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

O elemento x' é chamado *simétrico de x* para a operação $*$. Quando a operação é uma adição (+), o simétrico de x também é chamado *oposto de x* e indicado por $-x$. Quando a operação é uma multiplicação (·), o simétrico de x é chamado *inverso de x* e indicado por x^{-1}.

Exemplos e contra-exemplos

1º) *2* é um elemento simetrizável para a adição em $\mathbb{Z}$ e seu simétrico é *-2* pois:

$$(-2) + 2 = 0 = 2 + (-2)$$

2º) *2* é um elemento simetrizável para a multiplicação em $\mathbb{Q}$ e seu simétrico é $\frac{1}{2}$ pois:

$$\frac{1}{2} \cdot 2 = 1 = 2 \cdot \frac{1}{2}$$

0 não é simetrizável para a mesma operação pois não há elemento x' em $\mathbb{Q}$ tal que:

$$0 \cdot x' = 1 = x' \cdot 0$$

3º) 2 não é simetrizável para a multiplicação em $\mathbb{Z}$ pois não existe $x' \in \mathbb{Z}$ tal que $x' \cdot 2 = 1 = 2 \cdot x'$.

4º) $\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$ é simetrizável para a adição em $M_{2\times 2}(\mathbb{R})$ e seu simétrico é $\begin{pmatrix} -1 & -2 \\ -2 & -4 \end{pmatrix}$ pois:

$$\begin{pmatrix} -1 & -2 \\ -2 & -4 \end{pmatrix} + \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} + \begin{pmatrix} -1 & -2 \\ -2 & -4 \end{pmatrix}$$

5º) $\begin{pmatrix} 1 & 3 \\ -2 & -5 \end{pmatrix}$ é simetrizável para a multiplicação em $M_2(\mathbb{R})$ e seu simétrico é $\begin{pmatrix} -5 & -3 \\ 2 & 1 \end{pmatrix}$ pois:

$$\begin{pmatrix} -5 & -3 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 3 \\ -2 & -5 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ -2 & -5 \end{pmatrix} \cdot \begin{pmatrix} -5 & -3 \\ 2 & 1 \end{pmatrix}$$

$\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$ não é simetrizável para a mesma operação pois:

$$\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \cdot \begin{pmatrix} x & y \\ z & t \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \iff \begin{cases} x + 2z = 1 \\ y + 2t = 0 \\ 2x + 4z = 0 \\ 2y + 4t = 1 \end{cases}$$

e este sistema é incompatível.

6º) A função $f(x) = 2x + 1$ é bijetora de $\mathbb{R}$ em $\mathbb{R}$; logo existe a inversa de f, $f^{-1}(x) = \frac{x-1}{2}$, tal que $f^{-1} \circ f = i_{\mathbb{R}} = f \circ f^{-1}$. Podemos dizer que f é um elemento simetrizável de $\mathbb{R}^{\mathbb{R}}$ para a composição.

Já a função $g(x) = x^2$ não é uma bijeção de $\mathbb{R}$ em $\mathbb{R}$ e, por conseguinte, não é um elemento simetrizável para a mesma operação.

Proposição 7: Se a operação $*$ em E é associativa, tem elemento neutro e e um elemento $x \in E$ é simetrizável, então o simétrico de x é único.

Demonstração: Sejam x' e x'' simétricos de x. Temos:

$x' = e * x' = (x'' * x) * x' = x'' * (x * x') = x'' * e = x''$. ■

Proposição 8: Seja $*$ uma operação sobre E com elemento neutro e.

a) Se x é simetrizável, então x' também é e $(x')' = x$.

b) Se $*$ é associativa e $x, y \in E$ são simetrizáveis, então $x * y$ é simetrizável e $(x * y)' = y' * x'$

Demonstração

a) Sendo x' o simétrico de x temos $x' * x = x * x' = e$, o que mostra também que x é o simétrico de x'. Ou seja: $(x')' = x$.

b) Para provarmos que $y' * x'$ é o simétrico de $x * y$, devemos mostrar que:

(1) $(y' * x') * (x * y) = e$

(2) $(x * y) * (y' * x') = e$

De fato, temos:

(1) $(y' * x') * (x * y) = [(y' * x') * x] * y = [y' * (x' * x)] * y =$
$= (y' * e) * y = y' * y = e$

(2) analogamente. ■

Notação: Sendo $*$ uma operação sobre E com elemento neutro e, indica-se por $U_*(E)$ o conjunto dos elementos simetrizáveis de E para a operação $*$. Em símbolos:

$$U_*(E) = \{x \in E \mid \exists\ x' \in E : x' * x = e = x * x'\}$$

Por exemplo, temos:

a) $U_+(\mathbb{N}) = \{0\}$

b) $U_+(\mathbb{Z}) = \mathbb{Z}$

c) $U_\cdot(\mathbb{Z}) = \{1, -1\}$

d) $U_\cdot(\mathbb{R}) = \mathbb{R}^*$

e) $U_+(M_{m\times n}(\mathbb{R})) = M_{m\times n}(\mathbb{R})$

f) $U_\cdot(M_{2\times 2}(\mathbb{R})) = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \text{ e } ad - bc \neq 0\}$

g) $U_\circ(\mathbb{R}^{\mathbb{R}}) = \{f \in \mathbb{R}^{\mathbb{R}} \mid f \text{ é bijetora}\}$

Notemos que $U_*(E) \neq \phi$ pois necessariamente $e \in U_*(E)$ uma vez que $e * e = e$.

e) Elementos regulares

Definição 39: Dizemos que um elemento $a \in E$ é *regular* (ou simplificável) em relação à operação $*$ se:

$$a * x = a * y \Longrightarrow x = y \qquad (1)$$

e

$$x * a = y * a \Longrightarrow x = y \qquad (2)$$

quaisquer que sejam $x, y \in E$.

Valendo (1), dizemos que *a é regular à esquerda.* Valendo (2), *a é regular à direita.*

Observação: Se $*$ é comutativa, regular à esquerda significa regular à direita e vice-versa.

Exemplos e contra-exemplos

1º) *3* é regular para a adição em $\mathbb{N}$ pois:
$3 + x = 3 + y \Longrightarrow x = y$
para todos $x, y \in \mathbb{N}$.

2º) *3* é regular para a multiplicação em $\mathbb{Z}$ pois:
$3 \cdot x = 3 \cdot y \Longrightarrow x = y$
para todos $x, y \in \mathbb{Z}$.

3º) *0* não é regular para a multiplicação em $\mathbb{Z}$ pois:
$0 \cdot 2 = 0 \cdot 3$ e $2 \neq 3$.

4º) $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ é regular para a adição em $M_{2\times 2}(\mathbb{R})$ pois:

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} + \begin{pmatrix} x_1 & y_1 \\ z_1 & t_1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} + \begin{pmatrix} x_2 & y_2 \\ z_2 & t_2 \end{pmatrix} \Rightarrow \begin{pmatrix} x_1 & y_1 \\ z_1 & t_1 \end{pmatrix} = \begin{pmatrix} x_2 & y_2 \\ z_2 & t_2 \end{pmatrix}$$

5º) $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ não é regular para a multiplicação em $M_{2\times 2}(\mathbb{R})$ pois:

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix} \text{ e } \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix}$$

Proposição 9: Se a operação $*$ é associativa, tem neutro e e um elemento $a \in E$ é simetrizável, então a é regular.

Demonstração

Sejam x e y elementos quaisquer de E tais que $a*x = a*y$ e $x*a = y*a$. Temos:

(1) $a * x = a * y \Longrightarrow a' * (a * x) = a' * (a * y) \Longrightarrow$

$\Longrightarrow (a' * a) * x = (a' * a) * y \Longrightarrow e * x = e * y \Longrightarrow x = y$

e, analogamente:

(2) $x * a = y * a \Longrightarrow x = y$

portanto, *a* é regular. ■

Notação: Sendo $*$ uma operação sobre E, indica-se por $R_*(E)$ o conjunto dos elementos regulares de E para a operação $*$.

Por exemplo, temos:

a) $R_+(\mathbb{N}) = \mathbb{N}$

b) $R(\mathbb{Z}) = \mathbb{Z}^*$

c) $R_+(M_{mxn}(\mathbb{R}) = M_{mxn}(\mathbb{R})$

Notemos que se $*$ tem neutro em E, então $e \in R_*(E)$, portanto, $R_*(E) \neq \phi$. Observemos ainda que se, além disso, $*$ é associativa, $U_*(E) \subset R_*(E)$, conforme a proposição 9.

f) Propriedade distributiva

Definição 40: Sejam $*$ é Δ duas operações sobre E. Dizemos que Δ é *distributiva* em relação a $*$ se:

$x \Delta (y * z) = (x \Delta y) * (x \Delta z)$ (1)

$(y * z) \Delta x = (y \Delta x) * (z \Delta x)$ (2)

quaisquer que sejam $x, y, z \in E$.

Valendo (1), dizemos que Δ é *distributiva à esquerda* de $*$. Valendo (2), dizemos que Δ é *distributiva à direita* de $*$.

Observação: Se Δ é comutativa, então distributiva à esquerda ou à direita de $*$ são equivalentes.

Exemplos

1º) A multiplicação em $\mathbb{Z}$ é distributiva em relação à adição em $\mathbb{Z}$ pois:

$\forall x, y, z \in E : x.(y+z) = (x.y) + (x.z)$

2º) A multiplicação é distributiva em relação à adição em $M_n(\mathbb{R})$ pois:

$\forall A, B, C \in M_n(\mathbb{R}) : A.(B+C) = (A.B) + (A.C)$

$\forall A, B, C \in M_n(\mathbb{R}) : (B+C).A = (B.A) + (C.A)$

3º) A potenciação é distributiva à direita em relação à multiplicação em $\mathbb{N}$ pois:

$\forall x, y, z \in \mathbb{N} : (x.y)^n = x^n.y^n$

mas não é distributiva à esquerda pois:

$2^{3.4} \neq 2^3.2^4$.

5. PARTE FECHADA PARA UMA OPERAÇÃO

Definição 41: Seja $*$ uma operação sobre um conjunto $E \neq \phi$. Seja A um subconjunto não vazio de E. Dizemos que A é uma parte fechada de E para a operação $*$ se, e somente se, temos:

$x \in A \text{ e } y \in A \Longrightarrow x * y \in A$

para todos $x, y \in A$.

Exemplos

1º) Os racionais são uma parte fechada para a operação de adição sobre $\mathbb{R}$ pois $\mathbb{Q} \neq \phi$, $\mathbb{Q} \subset \mathbb{R}$ e $x, y \in \mathbb{Q} \Longrightarrow x + y \in \mathbb{Q}$, quaisquer que sejam *x* e *y*.

Notemos que os irracionais não são uma parte fechada para a adição sobre $\mathbb{R}$ pois, por exemplo, $\sqrt{2} \in \mathbb{R}-\mathbb{Q}$, $1-\sqrt{2} \in \mathbb{R}-\mathbb{Q}$ e $\sqrt{2}+(1-\sqrt{2}) \notin \mathbb{R}-\mathbb{Q}$.

2º) Os reais positivos são uma parte fechada para a multiplicação sobre $\mathbb{R}$ pois $\mathbb{R}_+^* \neq \phi$, $\mathbb{R}_+^* \subset \mathbb{R}$ e $x, y \in \mathbb{R}_+^* \Longrightarrow x.y \in \mathbb{R}_+^*$, quaisquer que sejam *x* e *y*.

3º) As funções bijetoras de $\mathbb{R}$ em $\mathbb{R}$ formam um subconjunto A fechado para a composição de funções de $\mathbb{R}^{\mathbb{R}}$ pois $A \neq \phi$, $A \subset \mathbb{R}^{\mathbb{R}}$ e $f, g \in A \Longrightarrow f \circ g \in A$, quaisquer que sejam *f* e *g*.

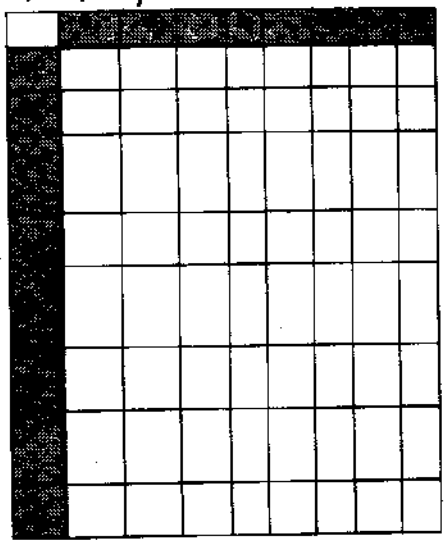
6. TÁBUA DE UMA OPERAÇÃO

Construção

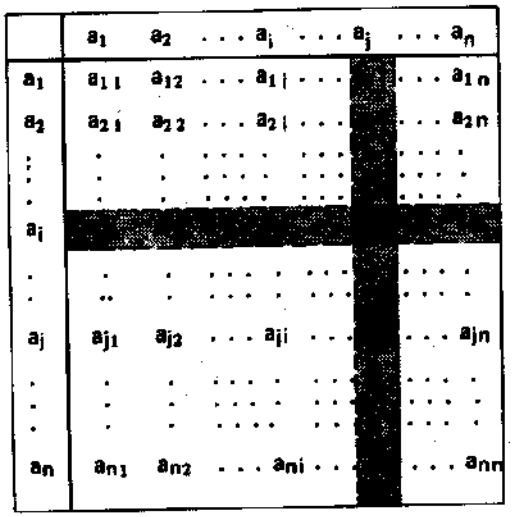
Seja $E = \{a_1, a_2, \ldots, a_n\}$ $(n \geq 1)$ um conjunto com n elementos. Cada operação sobre E é uma aplicação $f : E \times E \longrightarrow E$ que associa a cada par (a_i, a_j) o elemento $a_i * a_j = a_{ij}$.

Podemos indicar o correspondente a_{ij} para cada par (a_i, a_j) por meio de uma tabela de dupla entrada, construída como segue:

1º) Marcamos na linha fundamental e na coluna fundamental os elementos do conjunto E. Chamamos de i-ésima linha aquela que começa com a_i e de j-ésima coluna a que é encabeçada por a_j .



2º) Dado um elemento a_i na coluna fundamental e um elemento a_j na linha fundamental, na intersecção da linha i com a coluna j marcamos o composto a_{ij}.



Exemplos

1º) Tábua da operação de multiplicação sobre E = {-1, 0, 1}.

·	-1	0	1
-1	1	0	-1
0	0	0	0
1	-1	0	1

2º) Tábua da operação de intersecção sobre E = {A, B, C, D}, onde os conjuntos A, B, C, D são tais que $A \subset B \subset C \subset D$.

∩	A	B	C	D
A	A	A	A	A
B	A	B	B	B
C	A	B	C	C
D	A	B	C	D

3º) Tábua da operação mdc sobre E = {1, 3, 5, 15}, isto é, f(x, y) = = mdc (x, y).

mdc	1	3	5	15
1	1	1	1	1
3	1	3	1	3
5	1	1	5	5
15	1	3	5	15

4º) Tábua da operação de composição sobre E = $\{f_1, f_2, f_3\}$ onde as funções f_1, f_2, f_3 são assim descritas:

$f_1 = \{(a, a), (b, b), (c, c)\}$

$f_2 = \{(a, b), (b, c), (c, a)\}$

$f_3 = \{(a, c), (b, a), (c, b)\}$

∘	f_1	f_2	f_3
f_1	f_1	f_2	f_3
f_2	f_2	f_3	f_1
f_3	f_3	f_1	f_2

Propriedades

Vejamos agora como se pode estudar as propriedades de uma operação $*$ sobre $E = \{a_1, a_2, \ldots, a_n\}$, quando $*$ é dada por meio de uma tábua.

a) Associativa

É aquela cuja verificação exige maior trabalho. Pode ser feita de dois modos:

1º) Calculam-se todos os compostos do tipo $a_i * (a_j * a_k)$ com $i, j, k \in \{1, 2, \ldots, n\}$; calculam-se todos os compostos do tipo $(a_i * a_j) * a_k$, com $i, j, k \in \{1, 2, \ldots, n\}$. Notemos que este método exige o cálculo de $2n^3$ compostos.

2º) Encontra-se um conjunto F dotado de uma operação Δ que se sabe ser associativa, de tal forma que exista $f : E \longrightarrow F$ com as seguintes propriedades:

a) f é bijetora;

b) $f(x * y) = f(x) \Delta f(y)$ para todos $x, y \in E$.

Se isto ocorrer, então a lei $*$ também é associativa (verifique como exercício).

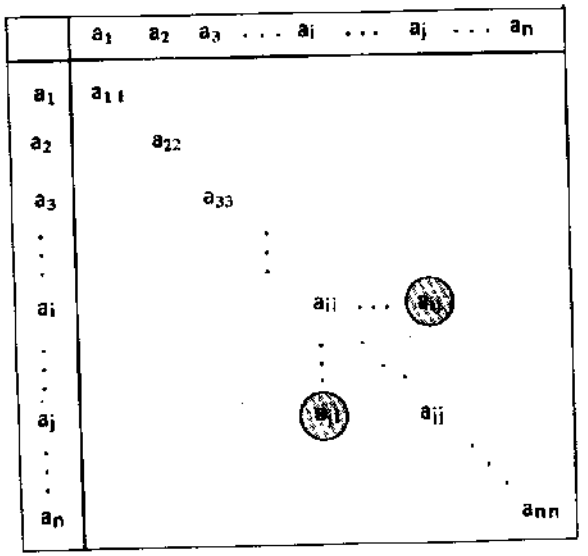
b) Comutativa

Chamamos de *diagonal principal* da tábua de uma operação o conjunto formado pelos compostos $a_{11}, a_{22}, a_{33}, \ldots, a_{nn}$.

Sabemos que uma operação é comutativa se:

$$a_i * a_j = a_j * a_i$$

isto é, se $a_{ij} = a_{ij}$ para quaisquer $i, j = 1, 2, 3, \ldots, n$.



Mas a_{ij} e a_{ji} ocupam posições simétricas relativamente à diagonal principal; portanto uma operação $*$ é comutativa desde que sua tábua seja simétrica em relação à diagonal principal, isto é, compostos colocados simetricamente em relação à diagonal são iguais.

Nos quatro exemplos dados há pouco, as operações são todas comutativas.

Um exemplo de operação não comutativa é dado pela tabela ao lado. Notemos que:

$b * c = a$ e $c * b = b$

*	a	b	c
a	a	b	c
b	b	c	a
c	c	b	a

c) Elemento neutro

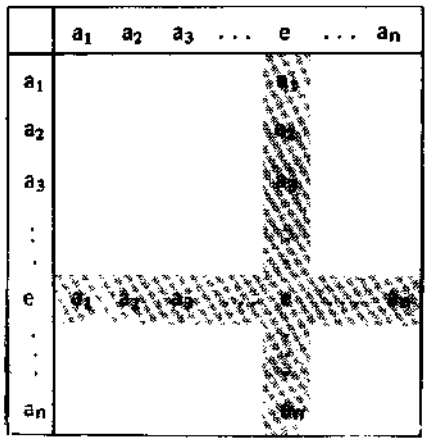
Sabemos que um elemento *e* é neutro para a operação $*$ quando:

(I) $e * x = x, \forall x \in E$ e (II) $x * e = x, \forall x \in E$

Da condição (I) decorre que a linha de *e* é igual a linha fundamental.

Da condição (II) decorre que a coluna de *e* é igual à coluna fundamental.

Assim, uma operação $*$ tem neutro desde que exista um elemento cuja linha e coluna são respectivamente iguais à linha e coluna fundamentais.



Nos quatro exemplos dados há pouco, as operações têm neutro que é 1, D, 15 e f_1 respectivamente.

Um exemplo de operação sem neutro é dado pela tábua ao lado. Notemos que a é neutro só à esquerda.

	a	b	c
a	a	b	c
b	c	a	b
c	b	a	c

d) Elementos simetrizáveis

Sabemos que um elemento $a_i \in E$ é simetrizável para a operação $*$ (que têm neutro e) quando existe um $a_j \in E$ tal que:

(I) $a_j * a_i = e$

e

(II) $a_i * a_j = e$

Da condição (II) decorre que a linha de a_i deve apresentar ao menos um composto igual a e.

Da condição (I) decorre que a coluna de a_i deve apresentar ao menos um composto igual a e.

*	a_1	a_2	...	a_i	...	a_j	...	a_n
a_1								
a_2								
⋮								
a_i						■		
⋮								
a_j				■				
⋮								
a_n								

Como $a_{ij} = a_{ji} = e$ decorre que o neutro deve figurar em posições simétricas relativamente à diagonal principal.

Assim, um elemento a_i é simetrizável quando o neutro figura ao menos uma vez na linha i e na coluna i da tábua, ocupando posições simétricas em relação à diagonal principal.

Por exemplo, a tábua ao lado define uma operação $*$ sobre $E = \{e, a_1, a_2, a_3, a_4\}$ que tem neutro e. Os elementos simetrizáveis de E são: e, a_1 e a_4.

*	e	a_1	a_2	a_3	a_4
e	e	a_1	a_2	a_3	a_4
a_1	a_1	a_2	a_3	a_4	e
a_2	a_2	a_3	a_4	a_1	a_2
a_3	a_3	a_4	a_1	a_2	a_1
a_4	a_4	e	a_3	a_4	a_2

e) Elementos regulares

Sabemos que um elemento $a \in E$ é regular em relação à operação $*$ quando:

(I) $x \neq y \Longrightarrow a * x \neq a * y$

e

(II) $x \neq y \Longrightarrow x * a \neq y * a$

onde x e y são elementos quaisquer de E.

Isto significa que a é regular quando, composto com elementos distintos (à esquerda deles ou à direita), produz resultados distintos.

Assim, um elemento a é regular quando na linha e na coluna de a não houver resultados iguais.

Por exemplo, a tábua ao lado define uma operação sobre $E = \{e, a, b, c, d\}$ onde os elementos regulares são e, a, c.

*	e	a	b	c	d
e	e	a	b	c	d
a	a	b	d	e	c
b	b	c	c	b	b
c	c	d	e	a	b
d	d	e	b	d	b

7. ADIÇÃO E MULTIPLICAÇÃO EM Z_m

Vamos definir aqui as operações de adição e multiplicação num conjunto Z_m $(m > 1)$ de classes de restos. Em seguida, mostraremos algumas propriedades, dessa operações.

Definições

Se $\overline{a} = \overline{a}_1 \in Z_m$ e $\overline{b} = \overline{b}_1 \in Z_m$, então $a \equiv a_1 \pmod m$ e $b \equiv b_1 \pmod m$, portanto, $a + b \equiv a_1 + b_1 \pmod m$ e $a \cdot b \equiv a_1 \cdot b_1 \pmod m$ e, conseqüentemente, $\overline{a + b} = \overline{a_1 + b_1}$ e $\overline{a \cdot b} = \overline{a_1 \cdot b_1}$. Isto torna lícitas as seguintes definições:

Definição 42: dadas duas classes $\overline{a}, \overline{b} \in Z_m$ chama-se soma $\overline{a} + \overline{b}$ a classe $\overline{a + b}$ (que é única, independentemente do representante tomado para $\overline{a}$ ou para $\overline{b}$).

Definição 43: dadas duas classes $\overline{a}, \overline{b} \in Z_m$ chama-se produto $\overline{a} \cdot \overline{b}$ a classe $\overline{a \cdot b}$ (que é única, independentemente do representante tomado para $\overline{a}$ ou para $\overline{b}$).

Assim, acabamos de definir duas operações sobre Z_m : uma adição tal que:

$$\overline{a} + \overline{b} = \overline{a + b}$$

e uma multiplicação tal que:

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

Propriedades da adição

i) Associativa

Sendo $\overline{a}, \overline{b}, \overline{c} \in Z_m$, temos:

$$\overline{a} + (\overline{b} + \overline{c}) = \overline{a} + \overline{b + c} = \overline{a + (b + c)} = \overline{(a + b) + c} = \overline{a + b} + \overline{c} = (\overline{a + b}) + \overline{c}$$

ii) Comutativa

Sendo $\overline{a}, \overline{b} \in Z_m$, temos:

$$\overline{a} + \overline{b} = \overline{a + b} = \overline{b + a} = \overline{b} + \overline{a}$$

iii) Elemento neutro

$\overline{a} + \overline{0} = \overline{a+0} = \overline{a}, \forall\ \overline{a} \in \mathbb{Z}_m$

portanto, $\overline{0}$ é o neutro da adição em $\mathbb{Z}_m$.

iv) Elementos simetrizáveis

$\overline{a} + \overline{m-a} = \overline{a+(m-a)} = \overline{m} = \overline{0},\ \forall\ \overline{a} \in \mathbb{Z}_m$

portanto, todo elemento de $\mathbb{Z}_m$ é simetrizável para a adição: o simétrico aditivo de $\overline{a}$ é $\overline{m-a}$.

Propriedades da multiplicação

i) Associativa

A prova fica como exercício.

ii) Comutativa

Idem.

iii) Elemento neutro

$\overline{a}.\overline{1} = \overline{a.1} = \overline{a},\ \forall\ \overline{a} \in \mathbb{Z}_m$

logo, $\overline{1}$ é o neutro da multiplicação em $\mathbb{Z}_m$.

iv) Elementos simetrizáveis

Provaremos que $\overline{a} \in \mathbb{Z}_m$ é simetrizável para a multiplicação se, e somente se, mdc (a, m) = 1.

Prova 1: $\overline{a} \in U_*(\mathbb{Z}_m) \Longrightarrow$ mdc (a, m) = 1

$\overline{a} \in U_*(\mathbb{Z}_m) \Longrightarrow (\ \exists\ \overline{b} \in \mathbb{Z}_m : \overline{a}.\overline{b} = \overline{1}) \Longrightarrow a.b \equiv 1 \pmod{m} \Longrightarrow$

$\Longrightarrow (\ \exists\ q \in \mathbb{Z} : ab - 1 = qm) \Longrightarrow ab - qm = 1$

Por outro lado, temos:

$d = \text{mdc}\ (a, m) \Longrightarrow (d \mid a \text{ e } d \mid m) \Longrightarrow d \mid (ab - qm) \Longrightarrow d \mid 1 \Longrightarrow d = 1.$

Prova 2: mdc (a, m) = 1 $\Longrightarrow \overline{a} \in U_*(\mathbb{Z}_m)$

mdc (a, m) = 1 $\Longrightarrow (\ \exists\ x_0, y_0 \in \mathbb{Z} : ax_0 + my_0 = 1) \Longrightarrow ax_0 - 1 = (-y_0)m \Longrightarrow$

$\Longrightarrow ax_0 \equiv 1 \pmod{m} \Longrightarrow \overline{a}.\overline{x_0} = \overline{1} \Longrightarrow \overline{a} \in U_*(\mathbb{Z}_m)$.

EXERCÍCIOS

101. Em cada caso abaixo, considere a operação $*$ sobre E e verifique se é associativa, se é comutativa, se existe elemento neutro e determine os elementos simetrizáveis.

a) $E = \mathbb{R}$ e $x * y = \dfrac{x+y}{2}$

b) $E = \mathbb{R}$ e $x * y = x$

c) $E = \mathbb{R}_+$ e $x * y = \sqrt{x^2 + y^2}$

d) $E = \mathbb{R}$ e $x * y = \sqrt[3]{x^3 + y^3}$

e) $E = \mathbb{R}^*$ e $x * y = \dfrac{x}{y}$

f) $E = \mathbb{R}_+$ e $x * y = \dfrac{x+y}{1+xy}$

g) $E = \mathbb{Z}$ e $x * y = x + y + x.y$

h) $E = \mathbb{Z}$ e $x * y = xy + 2x$

i) $E = \mathbb{Q}$ e $x * y = x + xy$

j) $E = \mathbb{Z}$ e $x * y = x + xy$

k) $E = \mathbb{R}$ e $x * y = x^2 + y^2 + 2xy$

l) $E = \mathbb{R}$ e $x * y = x + y - 2x^2y^2$

m) $E = \mathbb{N}$ e $x * y = \min(x, y)$

n) $E = \mathbb{R}$ e $x * y = \max(x, y)$

o) $E = \mathbb{Z}$ e $x * y = \text{mdc}\ (x, y)$

p) $E = \mathbb{N}$ e $x * y = \text{mdc}\ (x, y)$

q) $E = \mathbb{Z}$ e $x * y = \text{mmc}\ (x, y)$

r) $E = \mathbb{N}$ e $x * y = \text{mmc}\ (x, y)$

102. Em cada caso abaixo, está definida uma operação sobre $\mathbb{Z}\times\mathbb{Z}$. Verifique se é associativa, se é comutativa, se existe neutro e determine os elementos simetrizáveis.

a) $(a, b) * (c, d) = (ac, 0)$

b) $(a, b) \Delta (c, d) = (a + c, b + d)$

c) $(a, b) \perp (c, d) = (ac, ad + bc)$

d) $(a, b) \circ (c, d) = (a + c, bd)$

e) $(a, b) \times (c, d) = (ac - bd, ad + bc)$

103. Sendo $*$ a operação sobre $\mathbb{Z}^3$ dada pela lei $(a, b, c) * (d, e, f) = (ad, be, cf)$, provar que $*$ é associativa e tem neutro. Determinar $U_*(\mathbb{Z}^3)$.

104. Em que condições, sobre m e $n \in \mathbb{Z}$ a operação dada por $x*y = mx + ny$, sobre $\mathbb{Z}$,

a) é associativa? b) é comutativa? c) admite elemento neutro?

105. Consideremos a operação $*$ em $\mathbb{R}$ definida por $x * y = ax + by + cxy$, onde a, b e c são números reais dados. Determinar as condições para a, b e c de modo que $*$ seja associativa e tenha elemento neutro.

106. Determinar todos os elementos neutros à esquerda no conjunto $E = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$ para a operação de multiplicação.

107. Determinar $\mathbb{R}_*(E)$ para cada operação definida no exercício 101.

108. Determinar os elementos regulares de $\mathbb{Z}\times\mathbb{Z}$ para cada operação definida no exercício 102.

109. Mostrar que nenhum elemento de $\mathbb{R}$ é regular para a operação Δ assim definida: $x \Delta y = x^2 + y^2 + xy$.

110. Verifique se a lei dada por $(a, b) \Delta (c, d) = (ac, ad + bc)$ é distributiva em relação à lei $(a, b) + (c, d) = (a + c, b + d)$, tudo em $\mathbb{Z}\times\mathbb{Z}$.

111. Ache $m \in \mathbb{R}$ de modo que a lei definida por $x \Delta y = x + my$ (sobre $\mathbb{R}$) seja distributiva em relação a $x * y = x + y + xy$ (sobre $\mathbb{R}$).

112. Dizer quais dos subconjuntos de $\mathbb{Z}$ são fechados para a operação de adição.
a) $\mathbb{Z}_-$
b) $P = \{x \in \mathbb{Z} \mid x \text{ é par}\}$
c) $I = \{x \in \mathbb{Z} \mid x \text{ é ímpar}\}$
d) $m\mathbb{Z} = \{x \in \mathbb{Z} \mid m \text{ divide } x\}$ (m fixo).

113. Dizer quais dos seguintes subconjuntos de $\mathbb{Z}$ são fechados para a operação de multiplicação.
a) $\mathbb{Z}_-$ b) P c) I d) $m\mathbb{Z}$

114. Mostrar que $A = \{z \in \mathbb{C} \mid z = \cos\theta + i \cdot \text{sen}\,\theta\}$ é subconjunto de $\mathbb{C}$ fechado para a multiplicação.

115. Mostrar que $A = \left\{ \begin{pmatrix} \cos a & \text{sen } a \\ -\text{sen } a & \cos a \end{pmatrix} \mid a \in \mathbb{R} \right\}$ é subconjunto de $M_2(\mathbb{R})$ fechado para a multiplicação.

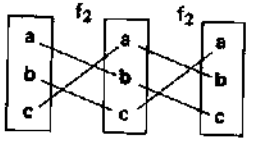
116. Em cada caso abaixo, está definida uma operação $*$ sobre E. Pede-se: fazer a tábua da operação, verificar se é comutativa e se existe neutro, determinar $U_*(E)$ e $R_*(E)$.
a) $E = \{1, 2, 3, 6\}$ e $x * y = \text{mdc}(x, y)$
b) $E = \{1, 3, 9, 27\}$ e $x * y = \text{mmc}(x, y)$
c) $E = \mathcal{P}(\{a, b\})$ e $x * y = x \cup y$
d) $E = \mathcal{P}(\{a, b\})$ e $x * y = x \cap y$
e) $E = \mathcal{P}(\{a, b\})$ e $x * y = (x \cup y) - (x \cap y)$
f) $E = \{\sqrt{3/2}, \sqrt[3]{5/2}, \sqrt[4]{7/2}\}$ e $x * y = \min\{x, y\}$
g) $E = \{3\sqrt{2}, \pi, 7/2\}$ e $x * y = \max\{x, y\}$
h) $E = \{1, i, -1, -i\}$ e $x * y = x \cdot y$
i) $E = \{0, 1, 2, 3\}$ e $x * y =$ resto da divisão em $\mathbb{Z}$ de $x + y$ por 4
j) $E = \{0, 1, 2, 3, 4\}$ e $x * y =$ resto da divisão em $\mathbb{Z}$ de $x \cdot y$ por 5.

117. Construir a tábua da operação de composição de funções em $E = \{f_1, f_2, f_3\}$ onde:
$f_1 = \{(a, a), (b, b), (c, c)\}$
$f_2 = \{(a, b), (b, c), (c, a)\}$
$f_3 = \{(a, c), (b, a), (c, b)\}$

Solução

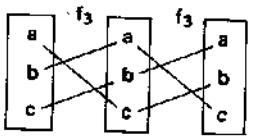
$f_1 \circ f_i = f_i = f_i \circ f_1$ pois f_1 é a identidade e, com isso, preenchemos a 1ª linha e a 1ª coluna.

$f_2 \circ f_2 = f_3$ pois



$f_2 \circ f_3 = f_1 = f_3 \circ f_2$ pois f_2 e f_3 são inversas entre si

$f_3 \circ f_3 = f_2$ pois



e, então, temos a tábua ao lado.

$\circ$	f_1	f_2	f_3
f_1	f_1	f_2	f_3
f_2	f_2	f_3	f_1
f_3	f_3	f_1	f_2

118. Construir a tábua da operação de composição de funções em $E = \{f_1, f_2, f_3, f_4\}$ onde :

$f_1 = \begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}$ $\quad f_2 = \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix}$

$f_3 = \begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix}$ $\quad f_4 = \begin{pmatrix} a & b & c & d \\ d & a & b & c \end{pmatrix}$

Em seguida calcular $f_2 \circ f_3 \circ f_4$, f_3^2, $(f_2 \circ f_4)^3$, $(f_3 \circ f_4)^{-1}$ e $f_2^{-1} \circ f_3^{-1}$.

Nota:

$f_2 = \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix}$, por exemplo, indica a função dada por: $a \longmapsto b$, $b \longmapsto c$, $c \longmapsto d$ e $d \longmapsto a$.

119. Seja E^E o conjunto das aplicações de E em E. A composição de aplicações é uma operação em E^E. Construir a tábua desta operação para $E = \{0, 1\}$.

120. Seja S(E) o conjunto das permutações de E (aplicações bijetoras de E em E). A composição de permutações é uma operação em S(E). Construir a tábua desta operação para $E = \{1, 2, 3\}$.

121. A partir das tábuas dos exercícios 119 e 120, verificar se as operações são comutativas, se existe neutro, que elementos são simetrizáveis e quais são regulares.

122. A partir de cada tábua abaixo, verifique se $*$ é comutativa, se existe neutro e que elementos são simetrizáveis.

a) $E = \{a, b, c, d\}$

*	a	b	c	d
a	c	d	a	b
b	d	c	b	a
c	a	b	c	d
d	b	a	d	c

b) $E = \{a, b, c, d\}$

*	a	b	c	d
a	c	a	d	b
b	a	b	c	d
c	b	c	d	a
d	d	d	a	c

c) $E = \{a, b, c, d, e, f, g, h\}$

*	a	b	c	d	e	f	g	h
a	a	b	c	d	e	f	g	h
b	b	c	d	a	f	g	h	e
c	c	d	a	b	g	h	e	f
d	d	a	b	c	h	e	f	g
e	e	f	g	h	a	b	c	d
f	f	g	h	e	b	c	d	a
g	g	h	e	f	c	d	a	b
h	h	e	f	g	d	a	b	c

123. Construir a tábua de uma operação $*$ sobre o conjunto $E = \{a, b, c, d\}$ de modo que:

I) seja comutativa;
II) *a* seja elemento neutro;
III) $U_*(E) = E$
IV) $R_*(E) = E$
V) $b * c = a$

124. Construir a tábua de uma operação Δ sobre o conjunto $E = \{e, a, b, c\}$ de modo que:

I) seja comutativa;
II) *e* seja elemento neutro;
III) $x * a = a, \forall x$
IV) $R_*(E) = E - \{a\}$

125. Dar um exemplo de operação sobre E em que todo elemento de E é regular, existe neutro e só ele é simetrizável.

126. Dar um exemplo de operação sobre E em que existe neutro e todos os elementos de E, com exceção do neutro, têm dois simétricos.

127. Dar um exemplo de operação em que o composto de dois elementos simetrizáveis não é simetrizável.

128. Dar um exemplo de operação não associativa nem comutativa mas que tem neutro.

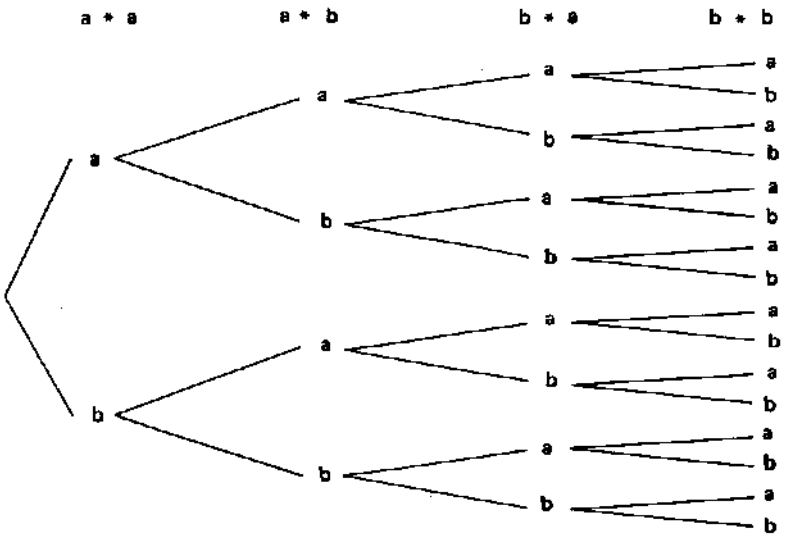
129. Seja $E = \mathcal{P}(\{a, b, c\})$. Qual é a condição sobre X e Y, com $X \in E$ e $Y \in E$, para que $\{X, Y\}$ seja fechado em relação à operação de intersecção sobre E?

130. Seja $*$ a operação sobre $E = \{1, 2, 3, 4, 6, 12\}$ definida por $x * y = \text{mmc}(x, y)$. Determinar os subconjuntos de E que têm três elementos e são fechados em relação a $*$.

131. Determinar todas as operações sobre o conjunto $E = \{a, b\}$.

Solução

Devemos determinar todas as aplicações de ExE em E, isto é, devemos atribuir um "valor" a cada um dos compostos a*a, a*b, b*a e b*b. Isto pode ser feito de 16 maneiras diferentes como mostra o diagrama abaixo



132. Mostrar que o número de operações sobre um conjunto finito com n elementos é $n^{(n^2)}$.

Sugestão: rever o exercício 54 deste capítulo.

133. Seja E um conjunto sobre o qual está definida uma operação $*$ que é associativa. Provar que:

a) $a \in E$ é regular à esquerda se, e somente se, $f : A \longrightarrow A$ tal que $f(x) = a*x$ é injetora;

b) $R_*(E)$ é fechado em relação a operação $*$;

c) se E é finito e $R_*(E) \neq \phi$, então existe elemento neutro para a operação $*$.

134. Seja E um conjunto munido de uma operação $*$ que admite elemento neutro e. Mostrar que esta operação é associativa e comutativa se, e somente se, $a * (b*c) = (a*c)*b$, quaisquer que sejam a, b e c em E.

135. Uma lei de composição interna $(x, y) \longmapsto x * y$ num conjunto $E \neq \phi$ é chamada totalmente não associativa se

$(\forall\ a, b, c)\ (a, b, c \in E \Longrightarrow (a * b) * c \neq a * (b * c))$

a) Mostre que tal lei não é comutativa.

b) Mostre que $(a, b) \longmapsto a^b$ é totalmente não associativa em $E = \{3, 4, \ldots\}$.

136. Seja $*$ uma operação sobre E que é associativa e tem neutro. Sendo A um subconjunto não vazio de E, indiquemos por C (A) o conjunto dos elementos $x \in E$ tais que $a*x = x*a$ para todo $a \in A$. Provar que:

a) C (A) é fechado em relação à operação $*$;

b) se $B \subset A$, então $C(B) \supset C(A)$;

c) $C(C(C(A))) = C(A)$.

Capítulo II

GRUPOS

§ 1º — GRUPOS E SUBGRUPOS

1. CONCEITO DE GRUPO

Definição 1: Sejam G um conjunto não vazio e $(x, y) \longmapsto x * y$ uma lei de composição interna em G. Dizemos que G é um *grupo* em relação a essa lei se, e somente se,

(a) $a * (b*c) = (a*b) * c, \forall\ a, b, c \in G$, isto é, *vale a propriedade associativa;*

(b) existe $e \in G$ de maneira que $a*e = e*a = a, \forall\ a \in G$, ou seja, *existe elemento neutro;*

(c) *todo elemento de G é simetrizável* em relação à lei considerada:

$\forall\ a \in G,\ \exists\ a' \in G \mid a * a' = a' * a = e$.

Às vezes, por simplificação de linguagem, diz-se apenas "G é um grupo" ou fala-se do "grupo G", o que pressupõe, evidentemente, uma lei de composição interna em G (com as propriedades citadas) sobre a qual não há nenhuma dúvida.

Notas

(i) Quando a lei de composição considerada for uma "adição" diremos que o grupo em questão é um "grupo aditivo" ao passo que se a lei for uma "multiplicação" nos referiremos a ele como "grupo multiplicativo".

(ii) Na maior parte da teoria sobre grupos a ser aqui desenvolvida usaremos a notação multiplicativa. Razão: é mais prática e, é claro, os resultados a serem obtidos independem do tipo de lei de composição interna a ser usada.

(iii) Se a lei que faz de G um grupo é dada por $(x, y) \longmapsto x * y$ também se costuma dizer que o par $(G, *)$, onde $*$ simboliza a lei, é um grupo.

2. GRUPOS COMUTATIVOS OU ABELIANOS

Definição 2: Dizemos que um grupo $(G, *)$ é *abeliano* ou *comutativo* se, e somente se, a lei $(x, y) \longmapsto x * y$ é comutativa, isto é,

$$a * b = b * a, \quad \forall\, a, b \in G.$$

Nota: Quando se desenvolve a teoria dos grupos comutativos a notação usada para indicar a lei de composição interna é, usualmente, a aditiva. A razão disso é que nos modelos mais importantes dessa situação (grupo abeliano) as operações são adições.

3. GRUPOS FINITOS — TÁBUA DE UM GRUPO FINITO

Um *grupo finito* é um grupo $(G, *)$ no qual o conjunto G é finito. O número de elementos de G, nesse caso, é chamado *ordem* do grupo G. A *tábua* de um grupo finito $(G, *)$ é a tábua da lei de composição considerada em G. Denotaremos a ordem de um grupo finito G por o(G).

Exemplo: É fácil verificar que $G = \{1, -1\}$ é um grupo em relação à multiplicação usual. Trata-se de um grupo finito de ordem 2 cuja tábua está ao lado.

*	1	-1
1	1	-1
-1	-1	1

4. ALGUNS GRUPOS IMPORTANTES

Veremos agora exemplos de grupos bastante importantes, seja pela freqüência com que aparecerão no curso deste texto em exemplos e exercícios, seja pelas suas aplicações dentro e fora da Matemática.

a) Grupo aditivo dos inteiros

Para a adição usual em $\mathbb{Z}$ vale, como já lembramos no capítulo zero, o seguinte

$$a + (b + c) = (a + b) + c$$
$$a + 0 = 0 + a = a$$
$$a + (-a) = (-a) + a = 0$$
$$a + b = b + a$$

Logo $(\mathbb{Z}, +)$ é um grupo abeliano. É o grupo aditivo dos inteiros.

b) Grupo aditivo dos racionais

Trata-se do grupo abeliano $(\mathbb{Q}, +)$ onde a adição considerada é a usual.

c) Grupo aditivo dos reais

É o grupo comutativo $(\mathbb{R}, +)$ onde a adição também é a usual.

d) Grupo aditivo dos complexos

Dados os números complexos $\alpha = a + bi$ e $\beta = c + di$ em $\mathbb{C}$ a soma de α com β é

$$\alpha + \beta = (a + c) + (b + d)i$$

O conjunto $\mathbb{C}$ é um grupo em relação à adição $(\alpha, \beta) \longmapsto \alpha + \beta$ assim definida. $(\mathbb{C}, +)$ é o grupo aditivo dos complexos.

e) Grupo multiplicativo dos racionais

O conjunto $\mathbb{Q}^*$ é fechado para a multiplicação usual em $\mathbb{Q}$ pois

$$(\forall\, a, b \in \mathbb{Q})\,(a \neq 0 \text{ e } b \neq 0 \Longrightarrow ab \neq 0)$$

Além disso tem-se o seguinte:

$$(ab)c = a(bc)$$
$$a \cdot 1 = 1 \cdot a = a$$
$$aa^{-1} = a^{-1}a = 1$$
$$ab = ba$$

Logo $(\mathbb{Q}^*, \cdot)$ é um grupo abeliano. É o grupo multiplicativo dos racionais.

f) Grupo multiplicativo dos reais

É o grupo $(\mathbb{R}^*, \cdot)$ cuja multiplicação é a habitual.

g) Grupo multiplicativo dos complexos

Dados os números complexos $\alpha = a + bi$ e $\beta = c + di$, ambos não nulos, então $\alpha\beta = (ac - bd) + (ad + bc)i$ também é um número complexo não nulo. Além disso tem-se o seguinte:

$$\alpha(\beta\gamma) = (\alpha\beta)\gamma$$
$$\alpha \cdot 1 = 1 \cdot \alpha = \alpha$$
$$\alpha \cdot \alpha^{-1} = \alpha^{-1}\alpha = 1$$
$$\alpha\beta = \beta\alpha$$

Destaque-se que $1 = 1 + 0i$ e que $\alpha^{-1} = \dfrac{-a}{a^2 + b^2} + \dfrac{b}{a^2 + b^2}\, i$ desde que $\alpha = a + bi \neq 0$. Logo $(\mathbb{C}^*, \cdot)$ também é um grupo abeliano. É o grupo multiplicativo dos complexos.

h) Grupo aditivo de matrizes

Indiquemos por $M_{m\times n}(\mathbb{Z})$ o conjunto das matrizes sobre $\mathbb{Z}$, m linhas e n colunas. A adição usual de matrizes desse conjunto é assim definida: se

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} b_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ b_{m1} & \cdots & b_{mn} \end{pmatrix}$$

então

$$A + B = \begin{pmatrix} a_{11} + b_{11} & \cdots & a_{1n} + b_{1n} \\ \cdots & \cdots & \cdots \\ a_{m1} + b_{m1} & \cdots & a_{mn} + b_{mn} \end{pmatrix}$$

Essa adição têm as seguintes propriedades de fácil verificação:

(i) $A + (B + C) = (A + B) + C$, $\forall\, A, B, C \in M_{m\times n}(\mathbb{Z})$

(ii) $A + 0 = 0 + A = A$, $\forall\, A \in M_{m\times n}(\mathbb{Z})$

onde $0 = \begin{pmatrix} 0 & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & 0 \end{pmatrix}$ (matriz nula)

(iii) Se $A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$

fazendo $\begin{pmatrix} -a_{11} & \cdots & -a_{1n} \\ \cdots & \cdots & \cdots \\ -a_{m1} & \cdots & -a_{mn} \end{pmatrix} = -A$

então $A + (-A) = (-A) + A = 0$ (matriz nula)

(iv) $A + B = B + A$, $\forall\, A, B \in M_{m\times n}(\mathbb{Z})$.

Logo $M_{m\times n}(\mathbb{Z})$ é um grupo abeliano em relação à adição assim definida. Tal grupo recebe o nome de grupo aditivo das matrizes sobre $\mathbb{Z}$.

Da mesma maneira se definem os grupos aditivos das matrizes sobre $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, ou seja, $(M_{m\times n}(\mathbb{Q}), +)$, $(M_{m\times n}(\mathbb{R}), +)$ e $(M_{m\times n}(\mathbb{C}), +)$.

i) Grupos lineares de grau n

Indiquemos por $M_n(\mathbb{Q})$ o conjunto das matrizes sobre $\mathbb{Q}$ de ordem n. Dadas as matrizes $A = (a_{ij})$ e $B = (b_{ij})$ de $M_n(\mathbb{Q})$ o produto de A por B é a matriz $AB = (c_{ij})$, onde

$$c_{ij} = \sum_{k=1}^{n} a_{ik}\, b_{kj} \quad (i, j = 1, \ldots, n).$$

Para essa multiplicação valem sempre, para todo $n \geqslant 1$ fixado, as seguintes propriedades:

(a) $A(BC) = (AB)C$

(b) $AI_n = I_nA = A$, $\forall\, A \in M_n(\mathbb{Q})$, onde

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

Mas não é para toda matriz $A \in M_n(\mathbb{Q})$ que existe uma outra matriz B, do mesmo conjunto, de modo que

$$AB = BA = I_n.$$

Por exemplo, se considerarmos a matriz

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

para toda matriz $B = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$

$AB = I_2 \implies x + z = 1,\ y + t = 0,\ 0 = 0$ e $0 = 1$ (absurdo).

Considerando contudo o subconjunto $GL_n(\mathbb{Q})$ das matrizes de $M_n(\mathbb{Q})$ que têm determinante não nulo, ou seja,

$$GL_n(\mathbb{Q}) = \{A \in M_n(\mathbb{Q}) \mid \det(A) \neq 0\}$$

e levando em conta que $\det(AB) = \det(A)\det(B)$, então $GL_n(\mathbb{Q})$ é fechado para a multiplicação de matrizes de $M_n(\mathbb{Q})$ pois

$$\det(A) \neq 0 \text{ e } \det(B) \neq 0 \implies \det(AB) = \det(A)\det(B) \neq 0.$$

Além disso, tem-se nesse conjunto o seguinte:

$(AB)C = A(BC)$, $\forall\, A, B, C \in M_n(\mathbb{Q})$

$I_n \in GL_n(\mathbb{Q})$, pois $\det(I_n) = 1$

Se $A \in GL_n(\mathbb{Q})$, então A^{-1} também é uma matriz de determinante não nulo uma vez que

$$1 = \det(I_n) = \det(AA^{-1}) = \det(A)\det(A^{-1}) \implies \det(A^{-1}) \neq 0.$$

Logo $GL_n(\mathbb{Q})$ é um grupo multiplicativo (em geral não abeliano). É chamado *grupo linear racional de grau n.*

Nota: Analogamente se definem os *grupos lineares reais* e os *grupos lineares complexos*, respectivamente

$$(GL_n(\mathbb{R}), \cdot) \quad \text{e} \quad (GL_n(\mathbb{C}), \cdot).$$

j) Grupos aditivos de classes de restos

Para todo $m > 1$, definimos a adição em $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ por

$$\overline{a} + \overline{b} = \overline{a+b}, \quad \forall\, \overline{a}, \overline{b} \in \mathbb{Z}_m,$$

isto no § 5 do capítulo 1.

Nesse mesmo parágrafo, mostramos que a adição assim definida em $\mathbb{Z}_m$ verifica as quatro propriedades que compõem a definição de grupo abeliano. Cada grupo $(\mathbb{Z}_m, +)$ $(\forall\, m > 1)$ é chamado *grupo aditivo das classes de restos módulo m.*

k) Grupos multiplicativos de classes de restos

O que vimos no § 5 do capítulo 1 nos permite concluir que $(\mathbb{Z}_m^*, \cdot)$, onde a multiplicação é dada por

$$\overline{a}\,\overline{b} = \overline{ab}$$

não é em geral um grupo. Nosso objetivo agora é mostrar que $(\mathbb{Z}_m^*, \cdot)$ é um grupo se, e somente se, m é um número primo $(m > 1)$.

$(\Longrightarrow)$ Suponhamos que $(\mathbb{Z}_m^*, \cdot)$ é um grupo e que m não é primo. Então existem dois números naturais r e s, ambos maiores do que 1, de modo que, $m = rs$. Desta igualdade resulta que

$$\overline{0} = \overline{m} = \overline{rs}$$

o que é absurdo pois $\overline{0} \notin \mathbb{Z}_m^*$.

$(\Longleftarrow)$ Tomemos $\overline{r}, \overline{s} \in \mathbb{Z}_m^*$. Se tivéssemos $\overline{rs} = \overline{0}$, então teríamos $rs \equiv 0 \pmod m$ o que equivale a dizer que $m \mid rs$. Como m é primo, então

$$m \mid r \quad \text{ou} \quad m \mid s$$

ou seja

$$\overline{r} = \overline{0} \quad \text{ou} \quad \overline{s} = \overline{0}$$

o que é impossível. Logo $\mathbb{Z}_m^*$ é fechado para a multiplicação definida em $\mathbb{Z}_m$.

Obviamente

$$\overline{a}\,(\overline{b}\,\overline{c}) = (\overline{a}\,\overline{b})\,\overline{c}, \quad \forall\, \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m^* \qquad \text{e} \qquad \overline{1} \in \mathbb{Z}_m^*$$

Por outro lado, tomando $\overline{a} \in \mathbb{Z}_m^*$ é claro que a não é múltiplo de m. Logo $\text{mdc}(a, m) = 1$. Isto nos permite concluir que $\overline{a}$ é inversível em $\mathbb{Z}_m$ (ver § 5 - cap. 1). Como o inverso de $\overline{a}$ obviamente não é nulo, então $\overline{a}$ admite simétrico multiplicativo em $\mathbb{Z}_m^*$.

Em resumo, para todo primo $m > 1$, $(\mathbb{Z}_m^*, \cdot)$ é um grupo. É claro que é abeliano. Cada $(\mathbb{Z}_m^*, \cdot)$ é chamado *grupo multiplicativo das classes de resto módulo m*, o que pressupõe naturalmente que m seja primo.

l) Grupos de permutações

(I) Seja E um conjunto não vazio. Indiquemos por S(E) o conjunto de todas as bijeções de E. Levando em conta o que já vimos no capítulo 1 a respeito de aplicações, podemos dizer que

$$(f, g) \longmapsto f \circ g, \quad \forall\, f, g \in S(E)$$

é uma lei de composição interna em S(E), associativa, com elemento neutro (a aplicação idêntica i_E) e, em relação à qual, todo elemento de S(E) é simetrizável: o simétrico de $f \in S(E)$ é f^{-1}, aplicação inversa de f.

O grupo $(S(E), \circ)$ é chamado grupo das permutações sobre E. Tal grupo só é comutativo quando E é formado por 1 ou por 2 elementos apenas (exercício).

(II) Se $E = \{1, 2, \ldots, n\}$, $n \geqslant 1$, tem-se um caso particular importante. S(E) passa a ser indicado por S_n e denominado *grupo simétrico de grau n.* A análise combinatória nos mostra que S_n é um grupo de ordem $n!$.

Um elemento $f \in S_n$ é normalmente indicado por

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$$

onde $i_r = f(r)$ $(r = 1, \ldots, n)$. Nesta notação não importa a ordem das colunas. Por exemplo, em S_3

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

Para efetuar a composição de dois elementos

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix} \qquad g = \begin{pmatrix} 1 & 2 & \ldots & n \\ j_1 & j_2 & \ldots & j_n \end{pmatrix}$$

de S_n procede-se assim

$$f \circ g = \begin{pmatrix} 1 & \ldots & i_r & \ldots & n \\ j_1 & \ldots & j_{i_r} & \ldots & j_n \end{pmatrix} \cdot \begin{pmatrix} 1 & \ldots & r & \ldots & n \\ i_1 & \ldots & i_r & \ldots & i_n \end{pmatrix} = \begin{pmatrix} \ldots & \ldots & \overline{r} & \ldots & \ldots \\ \ldots & \ldots & j_{i_r} & \ldots & \ldots \end{pmatrix}$$

pois $(f \circ g)(r) = f(g(r)) = f(i_r) = j_{i_r}$ $(r = 1, 2, \ldots, n)$.

Por exemplo, em S_4

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

Ainda de acordo com a mesma notação, se

$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$, então é claro que $f^{-1} = \begin{pmatrix} i_1 & i_2 & \ldots & i_n \\ 1 & 2 & \ldots & n \end{pmatrix}$

Exemplos

(1) Tábua de S_2

$$S_2 = \left\{ f_0 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix},\ f_1 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$$

$\circ$	f_0	f_1
f_0	f_0	f_1
f_1	f_1	f_0

(2) Tábua de S_3

$$S_3 = \left\{ f_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix};\ f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix};\ f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix};\right.$$

$$\left. f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix};\ f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix};\ f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}.$$

$\circ$	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_0	f_4	f_5	f_2	f_3
f_2	f_2	f_3	f_0	f_1	f_5	f_4
f_3	f_3	f_2	f_5	f_4	f_0	f_1
f_4	f_4	f_5	f_1	f_0	f_3	f_2
f_5	f_5	f_4	f_3	f_2	f_1	f_0

m) Grupos diedrais

(I) Grupos de Rotações

Consideremos um polígono regular de n vértices. Para facilitar as considerações que iremos fazer, imaginemos no plano do polígono um sistema ortogonal de coordenadas cartesianas de maneira que sua origem seja o centro do polígono e o eixo-x contenha um dos seus vértices o qual indicaremos pelo símbolo 1. Os vértices consecutivos desse serão indicados por 2, 3, . . . , n, respectivamente, no sentido anti-horário.

Nessas condições, as rotações em torno da origem e no sentido anti-horário segundo os ângulos de

$$0,\ \frac{2\pi}{n},\ 2.\frac{2\pi}{n},\ \ldots,\ (n-1).\frac{2\pi}{n} \quad \text{radianos}$$

transformam o polígono nele mesmo. Indiquemos por *e* a primeira dessas rotações e por *a* a segunda. Usando a notação multiplicativa para indicar a composição de duas rotações (duas rotações consecutivas), podemos dizer que o conjunto dessas n rotações é

$$R_n = \{e, a, a^2, \ldots, a^{n-1}\}$$

Obviamente $a^n = e$ o que significa que após efetuarmos n rotações de ângulo $\frac{2\pi}{n}$ o polígono volta à sua posição inicial. Além disso

$$a^{n+1} = a,\ a^{n+2} = a^2, \ldots$$

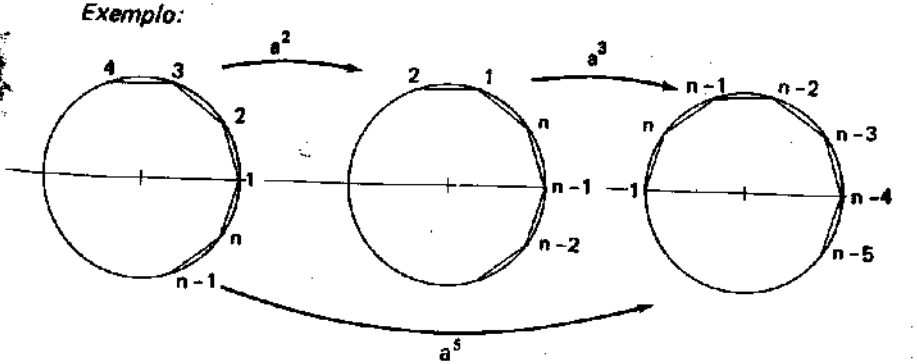
e também é evidente que $a^r a^s = a^{r+s}$ o que tem como conseqüência que R_n é fechado em relação à composição de rotações consideradas. É claro que vale a propriedade associativa:

$$a^r(a^s a^t) = a^r(a^{s+t}) = a^{r+(s+t)} = a^{(r+s)+t} = a^{r+s}a^t = (a^r a^s)a^t.$$

Por outro lado, como $a^r a^{n-r} = e$, então a^{n-r} é o simétrico, na composição de rotações, de a^r.

Assim R_n é um grupo cujo elemento neutro é *e* (polígono na posição inicial). R_n é chamado *grupo das rotações módulo n.*

Exemplo:

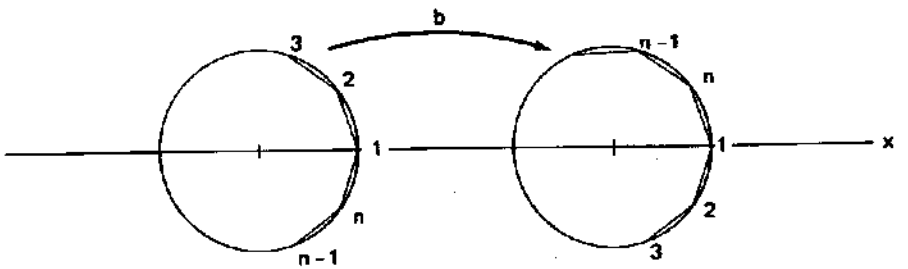


(II) *Grupos diedrais*

Indiquemos por b a reflexão em torno do eixo-x, conforme está indicado na figura abaixo. Temos então $b^2 = e$ (mantendo a notação do exemplo (I) acima). Seja D_{2n} o seguinte conjunto:

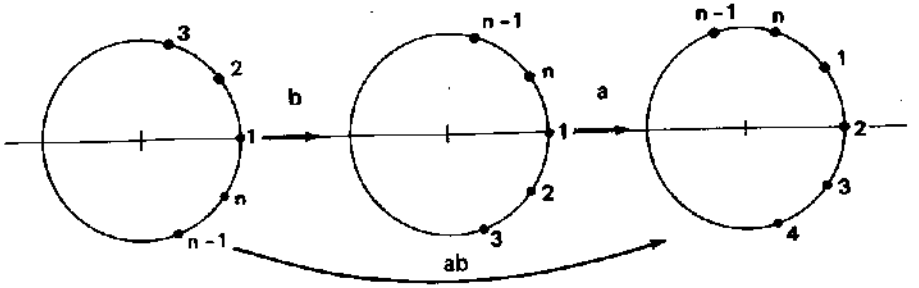
$$D_{2n} = \{e, a, \ldots, a^{n-1}, b, ba, \ldots, ba^{n-1}\}$$

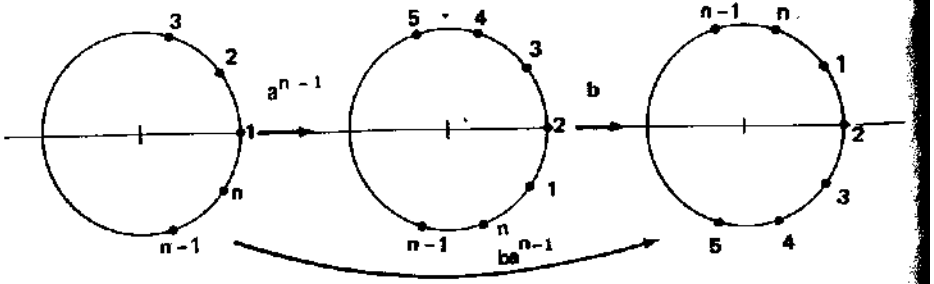
cujos elementos são as rotações de R_n e, ainda, estas seguidas da reflexão b.



Notemos que:

(i) $ab = ba^{n-1}$, conforme mostram as figuras a seguir





(ii) $a^r b = ba^{n-r}$ pois

$$a^r b = \underbrace{(aa \ldots a)}_{(r)} b = \underbrace{(aa \ldots a)}_{(r-1)} (ab) = a^{r-1}(ba^{n-1}) = (a^{r-1}b)\,a^{n-1} = \ldots =$$

$$= b\underbrace{(a^{n-1} \ldots a^{n-1})}_{(r)} = ba^{n-r}.$$

Como porém

$$a^{n-r}a^r = a^{rn} = (a^n)^r = e^r = e$$

então a^{rn-r} é o simétrico, na composição de rotações, de a^r. Donde

$$a^{rn-r} = a^{n-r}$$

Logo $a^r b = ba^{rn-r} = ba^{n-r}$.

(iii) O conjunto D_{2n} é fechado em relação à composição pois, por exemplo

$(ba^r)(ba^s) = b(a^r b)a^s = b(ba^{n-r})a^s = b^2 a^{n-r+s} = a^{(n+s)-r} \in D_{2n}$.

Mais precisamente, $(ba^r)(ba^s)$ é uma rotação. Fica como exercício a verificação de que $a^r(ba^s)$ não é uma rotação.

(iv) Para todo elemento de D_{2n} existe um simétrico em relação à composição, dentro do próprio conjunto D_{2n}. De fato.

Se o elemento considerado é de R_n já sabemos que isso é verdade.

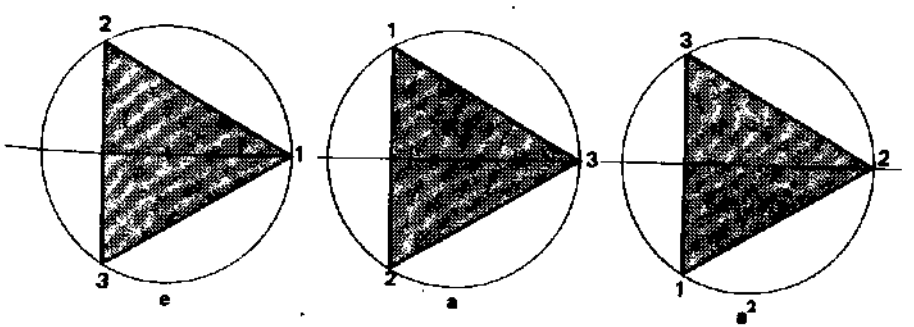
Caso contrário, basta observar que

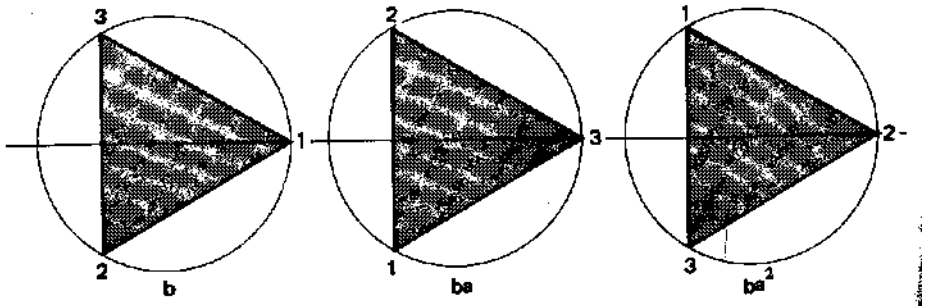
$(ba^r)(ba^r) = b(a^r b)a^r = b(ba^{n-r})a^r = b^2 a^n = ee = e$

ou seja, o simétrico de cada ba^r é o próprio ba^r, com $r = 0, 1, \ldots, n-1$ e $a^0 = e$, por definição.

Conclusão: O conjunto D_{2n} é um grupo que se denomina *Grupo Diedral de ordem 2n.*

Exemplo: Grupo diedral D_6





Tábua de D_6

	e	a	a^2	b	ba	ba^2
e	e	a	a^2	b	ba	ba^2
a	a	a^2	e	ba^2	b	ba
a^2	a^2	e	a	ba	ba^2	b
b	b	ba	ba^2	e	a	a^2
ba	ba	ba^2	b	a^2	e	a
ba^2	ba^2	b	ba	a	a^2	e

Note que, por exemplo,

$(ba)(ba^2) = b(ab)a^2 \overset{*}{=} b(ba^2)a^2 = b^2a^4 = a.$

* Usando a observação (i) feita atrás.

5. PROPRIEDADES IMEDIATAS DE UM GRUPO

Seja (G, $*$) um grupo. As propriedades que já provamos sobre leis de composição internas nos garantem que:

(a) o elemento neutro de (G, $*$) é único;

(b) existe um único simétrico para cada elemento $a \in G$;

(c) indicando por x' o simétrico de um elemento genérico $x \in G$:

$(\forall a, b)\ (a, b \in G \Longrightarrow (a * b)' = (b' * a')$

Por indução:

$(\forall a_1, \ldots, a_n)(a_1, \ldots, a_n \in G \Longrightarrow (a_1 * \ldots * a_n)' = a_n' * \ldots * a_1')$, onde

(d) $(\forall a)\ (a \in G \Longrightarrow (a')' = a)$

(e) todo elemento de G é regular em relação à lei $(x, y) \longmapsto x * y$.

Além disso, é de demonstração quase imediata, como veremos, a propriedade a seguir.

(f) Se $a, b \in G$, então a equação $a * x = b$, onde x é variável em G, admite uma única solução em G, a saber $a' * b$.

Como

$$a * (a' * b) = (a * a') * b = e * b = b$$

então $a' * b$ é solução. Por outro lado, se x_0 é solução da equação, segue deste fato que $a * x_0 = b$ é uma igualdade verdadeira. Daí

$$x_0 = e * x_0 = (a' * a) * x_0 = a' * (a * x_0) = a' * b.$$

6. SUBGRUPOS

Definição 3: Seja (G, $*$) um grupo. Dizemos que um subconjunto não vazio $H \subset G$ é um *subgrupo* de G se, e somente se,

(i) $\forall a, b \in H \Longrightarrow a * b \in H$ (isto é, H é fechado para a lei de composição interna de G);

(ii) (H, $*$) também é um grupo. (Aqui a lei de composição é a mesma de G, só que restrita a H.)

Proposição 1: Seja (G, $*$) um grupo. Para que um subconjunto não vazio $H \subset G$ seja um subgrupo de G é necessário e suficiente que

$$(\forall a, b)\ (a, b \in H \Longrightarrow a * b' \in H)$$

onde b' é o simétrico de b.

Demonstração: ($\Longrightarrow$) Indiquemos por e o elemento neutro de (G, $*$) e por e_h o elemento neutro de (H, $*$). Como

$$e_h * e_h = e_h = e_h * e$$

e todo elemento de G é regular em relação à lei considerada, tiramos daí que

$$e_h = e.$$

Tomemos agora um elemento $b \in H$ e indiquemos por b' e por b_h' os simétricos de b respectivamente no grupo G e no grupo H. Como porém

$$b_h' * b = e_h = e = b' * b$$

concluímos que $b_h' = b'$. Daí

$$a, b \in H \Longrightarrow a * b_h' \in H \Longrightarrow a * b' \in H$$

($\Longleftarrow$) Como $H \neq \phi$, existe $x_0 \in H$. Então a hipótese nos assegura que

$$x_0 * x_0' = e \in H.$$

Dado $b \in H$, usando a hipótese e a conclusão anterior de que $e \in H$, temos

$$e * b' = b' \in H.$$

Sejam agora $a, b \in H$. Devido ao que acabamos de deduzir podemos afirmar que $b' \in H$. Daí

$$a * (b')' = a * b \in H$$

em conseqüência de nossa hipótese. Logo H é fechado para a lei de composição interna de G. Por último, sendo $a, b, c \in H$, temos:

$$a, b, c \in H \Longrightarrow a, b, c \in G \Longrightarrow (a * b) * c = a * (b * c)$$

o que mostra, juntamente com o fechamento de H, a associatividade da lei de composição $(x, y) \longmapsto x * y$ em H. ■

Exemplos

(i) Consideremos o grupo multiplicativo dos reais: $(\mathbb{R}^*, \cdot)$. Mostremos que $H = \{x \in \mathbb{R} \mid x > 0\}$ é um subgrupo de $\mathbb{R}^*$. De fato:

$$a, b \in H \Longrightarrow (a \in \mathbb{R} \text{ e } a > 0) \text{ e } (b \in \mathbb{R} \text{ e } b > 0) \Longrightarrow (a \in \mathbb{R} \text{ e } b > 0)$$

$$\text{e } (b^{-1} \in \mathbb{R} \text{ e } b^{-1} > 0) \Longrightarrow ab^{-1} \in \mathbb{R} \text{ e } ab^{-1} > 0 \Longrightarrow ab^{-1} \in H.$$

(ii) Consideremos o grupo aditivo dos reais: $(\mathbb{R}, +)$. O conjunto $\mathbb{Z}$ dos inteiros é subgrupo de $\mathbb{R}$ porque obviamente

$$\forall a, b \in \mathbb{Z} \Longrightarrow a + (-b) = a - b \in \mathbb{Z}$$

Nota: Todo grupo G cujo elemento neutro indicamos por e admite pelo menos dois subgrupos: G e $\{e\}$. A verificação de que estes dois subconjuntos de G são subgrupos é imediata. Tais subgrupos são chamados *subgrupos triviais de G*.

EXERCÍCIOS

1. Mostrar que o conjunto $E = \{a + b \cdot \sqrt{2} \in \mathbb{R}^* \mid a, b \in \mathbb{Q}\}$ é um grupo multiplicativo abeliano.

2. Mostrar que $(\mathbb{R}, \Delta)$ é um grupo abeliano, quando Δ é definida por $x \Delta y = \sqrt[3]{x^3 + y^3}$.

3. Consideremos o conjunto dos números reais $\mathbb{R}$ munido da operação $*$ definida por $x * y = x + y - 3$. Mostrar que $(\mathbb{R}, *)$ é um grupo comutativo.

4. Verifique se $\mathbb{Z} \times \mathbb{Z}$ é grupo em relação a alguma das seguintes leis:
   a) $(a, b) \times (c, d) = (a + c, b + d)$
   b) $(a, b) \cdot (c, d) = (a \cdot c, b \cdot d)$

5. Sejam A um conjunto não vazio e $\mathbb{R}^A$ o conjunto das aplicações de A em $\mathbb{R}$. Definimos uma "adição" e uma "multiplicação" em $\mathbb{R}^A$ assim:
   $\forall f, g \in \mathbb{R}^A$: $(f + g)(x) = f(x) + g(x)$, $\forall x \in A$
   $(f \cdot g)(x) = f(x) \cdot g(x)$, $\forall x \in A$.
   Mostre que $(\mathbb{R}^A, +)$ é grupo. Por que $(\mathbb{R}^A, \cdot)$ não é grupo, em geral?

6. Mostrar que o conjunto das funções $f : \mathbb{R} \longrightarrow \mathbb{R}$ tais que $f(x) = ax + b$, com $a \neq 0$, é um grupo para a composição de funções.

7. Sendo $E \neq \phi$, mostrar que $(\mathcal{P}(E), \Delta)$ é um grupo.
   Nota: a operação Δ é assim definida:
   $x \Delta y = (x \cup y) - (x \cap y)$

8. Sejam $(G, *)$ e (J, Δ) grupos quaisquer. Mostre que $G \times J$ tem estrutura de grupo em relação à lei assim definida:
   $(x, y) \perp (x', y') = (x * x', y \Delta y')$, $\forall x, x' \in G$ e $\forall y, y' \in J$

9. Mostrar que só há um modelo de tábua para grupos de ordem 2.
   Sugestão: $G = \{e, a\}$, mostrar que $a * a = e$

10. Mostrar que só há um modelo de tábua para grupos de ordem 3.
    Sugestão: $G = \{e, a, b\}$, mostrar que $a * b = e$ e lembrar que $R(G) = G$.

11. Mostrar que cada uma das tábuas abaixo define uma operação que confere ao conjunto $E = \{e, a, b, c\}$ uma estrutura de grupo.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

(grupo de Klein)

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

(grupo cíclico de ordem 4)

12. Se $G = \{e, a, b, c\}$ é um grupo em relação à operação dada tabela abaixo, complete-a.

	e	a	b	c
e	e	a	b	c
a	a			
b	b	c		
c	c	e		

13. Sejam as aplicações F_1, F_2, F_3, F_4 de $\mathbb{R}^2$ em $\mathbb{R}^2$ definidas da seguinte maneira: $F_1(x, y) = (x, y)$, $F_2(x, y) = (-x, y)$, $F_3(x, y) = (x, -y)$ e $F_4(x, y) = (-x, -y)$. Se $G = \{F_1, F_2, F_3, F_4\}$, mostrar que $(G, \circ)$ é um grupo. Obter $F \in G$ tal que $F_1 \circ F_2 \circ F \circ F_3 = F_4^{-1}$.

14. Construir a tábua do grupo das rotações R_4.

15. Construir a tábua do grupo das rotações R_6.

16. Construir a tábua do grupo diedral de ordem 8.

17. Construir a tábua do grupo diedral de ordem 10.

18. Construir a tábua de um grupo $G = \{e, a, b, c, d, f\}$, de ordem 6, sabendo que:
   I. G é abeliano;
   II. o neutro é e;
   III. $a * f = b * d = e$
   IV. $a * d = b * c = f$
   V. $a * c = b * b = d$
   VI. $c * d = a$

19. Sejam G um grupo multiplicativo e a, b, c elementos de G. Provar que $(abc)^{-1} = c^{-1}b^{-1}a^{-1}$. Obter $x \in G$ tal que $abc * b = c$.

20. Mostrar que se x é elemento de um grupo multiplicativo e $xx = x$, então x é o elemento neutro.

21. Se G é um grupo multiplicativo e $xx = 1, \forall x \in G$, então G é abeliano.
   Sugestão: $(xy)^2 = 1$

22. Mostrar que se G é um grupo multiplicativo e se o conjunto G é finito e com um número par de elementos, então existe um elemento $x \neq 1$ em G tal que $x = x^{-1}$. (1 é o elemento neutro)
   Sugestão: $G = A \cup B$, $A = \{x \in G \mid x \neq x^{-1}\}$ e $B = \{x \in G \mid x = x^{-1}\}$

23. Seja G um conjunto finito e munido de uma operação $*$ que é associativa. Mostrar que se a operação $*$ satisfaz as duas leis do cancelamento, então $(G, *)$ é um grupo.

24. Verifique se são subgrupos:
   a) $\{x \in \mathbb{Q} \mid x > 0\}$, de $(\mathbb{Q}^*, \cdot)$
   b) $\left(\frac{1+2m}{1+2n} \mid m, n \in \mathbb{Z}\right)$, de $(\mathbb{Q}^*, \cdot)$
   c) $\{\cos\theta + i \operatorname{sen}\theta \mid \theta \in \mathbb{Q}\}$, de $(\mathbb{C}^*, \cdot)$
   d) $\{0, \pm 2, \pm 4, \ldots\}$, de $(\mathbb{Z}, +)$
   e) $\{0, \pm 2, \pm 4, \ldots\}$, de grupo $(\mathbb{Q} - \{1\}, *)$ onde $*$ está definida como $x * y = x + y - xy$

   f) $\{z \in \mathbb{C} \mid |z| = 1\}$, de $(\mathbb{C}^*, \cdot)$
   g) $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, de $(\mathbb{R}, +)$
   h) $\{a + b\sqrt{2} \in \mathbb{R}^* \mid a, b \in \mathbb{Q}\}$, de $(\mathbb{R}^*, \cdot)$
   i) $\{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Q}\}$, de $(\mathbb{R}, +)$
   j) $\{a + b\sqrt[3]{2} \in \mathbb{R}^* \mid a, b \in \mathbb{Q}\}$ de $(\mathbb{R}^*, \cdot)$

25. Mostrar que as matrizes do tipo $\begin{pmatrix} \cos a & \operatorname{sen} a \\ -\operatorname{sen} a & \cos a \end{pmatrix}$, com $a \in \mathbb{R}$, constituem um subgrupo do grupo multiplicativo das matrizes reais e inversíveis, do tipo 2×2.

26. Mostrar que as matrizes do tipo $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, com $a, b \in \mathbb{R}$ e não nulos simultâneamente, constituem um subgrupo do grupo linear $GL_2(\mathbb{R})$.

27. O conjunto $\mathbb{R}^n$, $\forall n \in \mathbb{Z}$, $n \geq 1$, é definido assim: $\mathbb{R}^n = \{(a_1, \ldots, a_n) \mid a_i \in \mathbb{R}\}$
   a) Mostre que $\mathbb{R}^n$ tem uma estrutura de grupo em relação à "adição".
   $(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$
   b) Verifique se são subgrupos de $(\mathbb{R}^n, +)$:
   $H_1 = \{(a_1, \ldots, a_n) \in \mathbb{R}^n \mid a_1 + \ldots + a_n = 0\}$
   $H_2 = \{(a_1, \ldots, a_n) \in \mathbb{R}^n \mid a_1 \in \mathbb{Z}\}$
   $H_3 = \{(a_1, \ldots, a_n) \in \mathbb{R}^n \mid a_1 \geq a_2 \geq \ldots \geq a_n\}$.

28. Seja G um grupo finito. Mostre que $H \subset G$, $H \neq \phi$, é subgrupo de G se, e somente se $a, b \in H \implies a * b \in H$.

29. Determinar todos os subgrupos do grupo aditivo $\mathbb{Z}_4$.

30. Seja $E = \{e, a, b, c, d, f\}$ munido da operação $\odot$ dada pela seguinte tábua:

$\odot$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	c	d	f	e
b	b	c	d	f	e	a
c	c	d	f	e	a	b
d	d	f	e	a	b	c
f	f	e	a	b	c	d

   1º) Admitindo a propriedade associativa, mostrar que $(E, \odot)$ é um grupo comutativo.
   2º) Obter os subgrupos de E com ordem 2 ou 3.

31. Seja $E = \{e, a, b, c, d, f\}$ munido da operação Δ dada pela seguinte tábua:

Δ	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

1º) Admitindo a propriedade associativa, provar que (E, Δ) é um grupo não comutativo

2º) Obter os subgrupos de E com ordem 2 ou 3.

32. Mostre que $H \subset \mathbb{Z}$ é subgrupo do grupo aditivo $\mathbb{Z}$ se, e somente se, $\exists\ m \in H$ de modo que $H = \{km \mid k \in \mathbb{Z}\}$.

Nota: Indica-se por $m\mathbb{Z}$ o subgrupo $\{km \mid k \in \mathbb{Z}\}$. Assim
$2\mathbb{Z} = (-2)\mathbb{Z} = \{0, \pm 2, \pm 4, \ldots\}$, $3\mathbb{Z} = (-3)\mathbb{Z} = \{0, \pm 3, \pm 6, \ldots\}$

33. Provar que se H_1 e H_2 são subgrupos de um grupo G, então $H_1 \cap H_2$ é um subgrupo de G.

34. Provar que se H_1 e H_2 são subgrupos de um grupo G, então $H_1 \cup H_2$ é subgrupo de G se, e somente se, $H_1 \subset H_2$ ou $H_1 \supset H_2$.

35. Seja G um grupo e a um elemento de G. Provar que $N(a) = \{x \in G \mid ax = xa\}$ é um subgrupo de G.

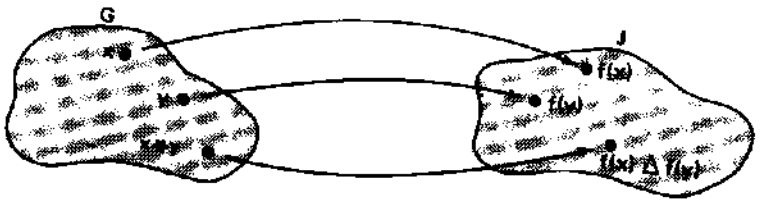
§ 2º — HOMOMORFISMOS E ISOMORFISMOS

1. HOMOMORFISMOS

Sejam $(G, *)$ e (J, Δ) grupos quaisquer. Quando se consideram aplicações

$$f : G \longrightarrow J$$

não pode ser ignorada, em geral, a existência das operações que dão a esses conjuntos as estruturas de grupo consideradas. Nessas condições interessam, em particular, para a teoria dos grupos, as aplicações que "preservam" essas operações no sentido que o diagrama abaixo nos mostra



Ou seja

$$f(x * y) = f(x) \Delta f(y), \ \forall\ x, y \in G.$$

Isso significa que quando se toma um par (x, y) qualquer em $G \times G$, obtém-se o mesmo elemento de J quer se ache $f(x * y)$, quer se considere o par $(f(x), f(y)) \in J \times J$ e com ele se calcule $f(x) \Delta f(y)$.

Essa idéia pode ser visualizada também no seguinte diagrama

$$\begin{array}{ccc} (x, y) & \longrightarrow & x * y \\ \downarrow & & \downarrow \\ (f(x), f(y)) & \longrightarrow & f(x) \Delta f(y) = f(x * y) \end{array}$$

Definição 4: Dados dois grupos $(G, *)$ e (J, Δ), dizemos que uma aplicação $f : G \longrightarrow J$ é um *homomorfismo* de G em J, se, e somente se,

$$(\forall\ a, b \in G)\ (f(a * b) = f(a) \Delta f(b)).$$

Um homomorfismo do grupo G nele próprio é chamado *endomorfismo* de G. Se $f : G \longrightarrow J$ é um homomorfismo de grupos e se f é injetora (resp., sobrejetora), então f recebe o nome de *monomorfismo* (resp., *epimorfismo*) de G em J.

Exemplos

1) A aplicação $f : \mathbb{Z} \longrightarrow \mathbb{C}^*$ dada por $f(m) = i^m$, $\forall\ m \in \mathbb{Z}$, é um homomorfismo de $(\mathbb{Z}, +)$ em $(\mathbb{C}^*, \cdot)$ pois

$$(\forall\ m, n \in \mathbb{Z})\ (f(m+n) = i^{m+n} = i^m i^n = f(m) \cdot f(n))$$

Observemos que f não é nem um monomorfismo (por exemplo, $f(0) = f(4) = f(8) = \ldots = 1$) e nem epimorfismo (o conjunto imagem de f se reduz aos elementos $1, -1, i, -i$).

2) $f : \mathbb{R}_+^* \longrightarrow \mathbb{R}$, dada por $f(x) = \log(x)$, $\forall\ x \in \mathbb{R}_+^*$, é um homomorfismo de $(\mathbb{R}_+^*, \cdot)$ em $(\mathbb{R}, +)$ uma vez que

$$(\forall\ a, b \in \mathbb{R}_+^*)\ (f(ab) = \log(ab) = \log(a) + \log(b) = f(a) + f(b)).$$

Observemos que f é tanto monomorfismo como epimorfismo porque a função logarítmo é tanto injetora como sobrejetora.

3) $f : \mathbb{C}^* \longrightarrow \mathbb{R}_+^*$ dada por $f(z) = |z|$ é um epimorfismo. De fato:

$$(\forall\ z_1, z_2 \in \mathbb{C}^*)\ (f(z_1 z_2) = |z_1 z_2| = |z_1|\,|z_2| = f(z_1) f(z_2)).$$

Além disso, como para todo $c \in \mathbb{R}_+^*$, $|c| = c$, podemos afirmar que f é sobrejetora.

2. PROPOSIÇÕES SOBRE HOMOMORFISMOS

Nas proposições que provaremos a seguir usaremos a notação multiplicativa para indicar as leis de composição internas dos grupos que estarão em jogo. Nosso objetivo com isso é o de simplificar as notações apenas.

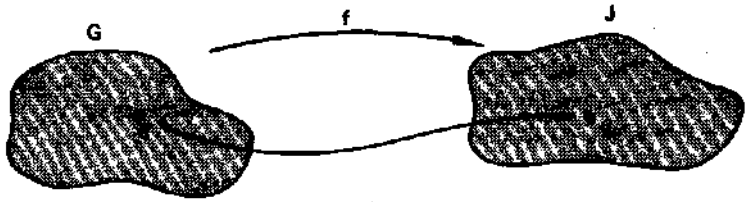
Sejam $(G, \cdot)$ e $(J, \cdot)$ dois grupos cujos elementos neutros indicaremos por e e u, respectivamente, e $f : G \longrightarrow J$ um homomorfismo.

Proposição 2: $f(e) = u$

Demonstração: $uf(e) = f(e) = f(ee) = f(e)f(e)$

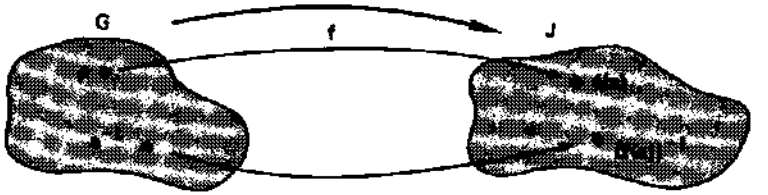
$u = f(e)$

(pois todo elemento de um grupo é regular). ■



Proposição 3: $(\forall\ a \in G)\ (f(a^{-1}) = (f(a))^{-1})$.

Demonstração:



$f(a)\,(f(a))^{-1} = u = f(e) = f(aa^{-1}) = f(a)f(a^{-1})$

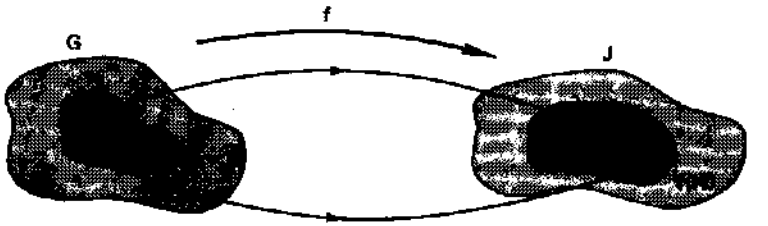
$(f(a))^{-1} = f(a^{-1})$

(Mesmo motivo da proposição 2). ■

Proposição 4: Se H é um subgrupo de G, então f(H) é um subgrupo de J.

Demonstração: Lembremos de início que $f(H) = \{f(x) \mid x \in H\}$.

a) $e \in H \Longrightarrow f(e) = u \in f(H) \Longrightarrow f(H) \neq \phi$



b) $c, d \in f(H) \Longrightarrow (\exists\ a, b \in H \mid c = f(a)$ e $d = f(b)) \Longrightarrow cd^{-1} = f(a)(f(b))^{-1} = f(a)f(b^{-1}) = f(ab^{-1})$. Como $ab^{-1} \in H$, pois H é subgrupo de G, então $cd^{-1} \in f(H)$. ■

Nota: A proposição que acabamos de provar pode assim ser interpretada: um homomorfismo de G em J transforma os subgrupos de G em subgrupos de J. Em particular Im(f) é um subgrupo de J.

Proposição 5: Sejam $(G, \cdot)$, $(J, \cdot)$ e $(L, \cdot)$ grupos quaisquer, $f: G \longrightarrow J$ e $g: J \longrightarrow L$, homomorfismos de grupos. Então $g \circ f : G \longrightarrow L$ também é um homomorfismo de grupos.

Demonstração: $(\forall a, b \in G)((g \circ f)(ab) = g(f(ab)) = g(f(a)f(b)) = g(f(a))g(f(b)) = (g \circ f)(a)(g \circ f)(b))$. ■

Corolários

I) Se f e g são monomorfismos, então $g \circ f$ também o é.

Demonstração: Basta lembrar que a composta de duas aplicações injetoras também é uma aplicação injetora. ■

II) Se f e g são epimorfismos, então $g \circ f$ também o é.

Demonstração: imediata.

3. NÚCLEO DE UM HOMOMORFISMO

Definição 5: Sejam $(G, *)$ e (J, Δ) grupos e $f : G \longrightarrow J$ um homomorfismo. Chama-se *núcleo* de f e denota-se por N(f) ou Ker(f) o seguinte subconjunto de G:

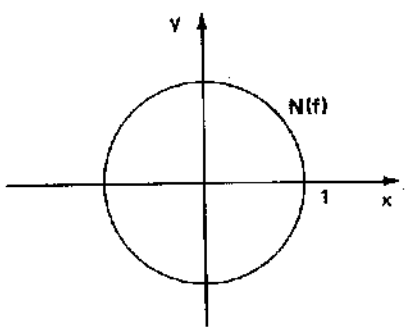
$$N(f) = \{x \in G \mid f(x) = u\},$$

onde u indica o elemento neutro de J.

Exemplos

1) Achemos o núcleo do homomorfismo $f : \mathbb{Z} \longrightarrow \mathbb{C}$ dado por $f(m) = i^m$.
   $N(f) = \{m \in \mathbb{Z} \mid i^m = 1\} = \{0, \pm 4, \pm 8, \ldots\}$
2) O núcleo do homomorfismo $f : \mathbb{R}_+^* \longrightarrow \mathbb{R}$ dado por $f(x) = \log(x)$ é
   $N(f) = \{x \in \mathbb{R}_+^* \mid \log(x) = 0\} = \{1\}$.
3) Determinemos o núcleo de $f : \mathbb{C}^* \longrightarrow \mathbb{R}_+^*$ definido por $f(z) = |z|$.
   $N(f) = \{z \in \mathbb{C}^* \mid |z| = 1\} = \{x + yi \in \mathbb{C}^* \mid x^2 + y^2 = 1\}$.

Logo o núcleo de f neste caso é o conjunto dos números complexos cujos afixos, num plano complexo, formam a circunferência de raio unitário e centro na origem.



Proposição 6: Seja $f : G \longrightarrow J$ um homomorfismo de grupos. Então: a) N(f) é um subgrupo de G; b) f é um monomorfismo se, e somente se $N(f) = \{e\}$ (e = el. neutro de G).

Demonstração: (a) Como $f(e) = u$, então $e \in N(f)$ o que mostra que $N(f) \neq \phi$. Por outro lado, se $a, b \in N(f)$, então $f(a) = f(b) = u$. Donde

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)(f(b))^{-1} = uu^{-1} = u.$$

Isto nos garante que $ab^{-1} \in N(f)$.

(b) $(\Longrightarrow)$ $a \in N(f) \Longrightarrow f(a) = u = f(e)$. Como f é injetora, então $a = e$.

$(\Longleftarrow)$ $\forall a, b \in G$, $f(a) = f(b) \Longrightarrow f(a)(f(b))^{-1} = u \Longrightarrow f(ab^{-1}) = u \Longrightarrow$
$\Longrightarrow ab^{-1} \in N(f) = \{e\} \Longrightarrow ab^{-1} = e \Longrightarrow a = b$. ■

Exemplo

Podemos concluir, com base na proposição anterior, que dos três exemplos já dados de homomorfismos de grupos é monomorfismo apenas o segundo, ou seja, a função logarítmo.

4. ISOMORFISMOS DE GRUPOS

Consideremos os grupos $G = \{1, -1\}$ (multiplicativo) e $J = S_2 = \left\{ u = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, v = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$. Observando as tábuas

·	1	-1
1	1	-1
-1	-1	1

∘	u	v
u	u	v
v	v	u

verificamos que, salvo o "nome" dos elementos e das operações em jogo, G e J comportam-se como se fossem o mesmo grupo.

Algebricamente esse fato se traduz pela existência de uma bijeção $f : G \longrightarrow J$ dada por $f(1) = u$ e $f(-1) = v$ que é também um homomorfismo de grupos pois

$$1 \cdot 1 = 1 \overset{f}{\longmapsto} u = u \circ u$$
$$1 \cdot (-1) = -1 \longmapsto v = u \circ v$$
$$(-1) \cdot (-1) = 1 \longmapsto u = v \circ v$$

A aplicação f, digamos, simplesmente troca os "nomes" dos elementos do grupo G: o 1 passa a se chamar u e o -1 passa a se chamar v. Podemos considerar os grupos em questão como indistintos sob o ponto de vista algébrico. Posteriormente veremos que todos os grupos de ordem 2 podem ser considerados indistintos segundo as considerações anteriores. *

Da idéia que acabamos de esboçar surge a definição a seguir.

Definição 6: Sejam $(G, *)$ e (J, Δ) grupos genéricos. Dizemos que uma aplicação $f: G \longrightarrow J$ é um *isomorfismo* do grupo G no grupo J se, e somente se,

a) f é bijetora;

b) f é um homomorfismo de grupos.

Se G = J, um isomorfismo $f: G \longrightarrow G$ chama-se *automorfismo* de G.

Exemplo

A função $f: \mathbb{R}_+^* \longrightarrow \mathbb{R}$ dada por $f(x) = \log(x)$, $\forall\, x \in \mathbb{R}$, é homomorfismo, conforme já foi provado, e é bijetora. Logo é um isomorfismo de $(\mathbb{R}_+^*, \cdot)$ em $(\mathbb{R}, +)$.

Nota: É claro que todas as proposições já provadas para homomorfismos também valem para isomorfismos. A proposição a seguir é específica dos isomorfismos.

Proposição 7: Se f é um isomorfismo do grupo G no grupo J, então f^{-1} é um isomorfismo do grupo J no grupo G.

Demonstração: Faremos a demonstração usando a notação multiplicativa para indicar as leis de composição, tanto de G como de J, o que não acarreta nenhuma perda de generalidade.

Como f é bijetora, então f^{-1} também é bijetora, conforme já provamos no capítulo anterior.

Sejam $y_1 = f(x_1) \in J$ e $y_2 = f(x_2) \in J$. Temos:

$f^{-1}(y_1 \cdot y_2) = f^{-1}(f(x_1) \cdot f(x_2)) = f^{-1}(f(x_1 x_2)) = x_1 x_2 = f^{-1}(y_1) \cdot f^{-1}(y_2)$. ■

Notas: 1) Quando existe um isomorfismo $f: G \longrightarrow J$, também existe um isomorfismo de J em G que é a aplicação f^{-1}. Por isso dizemos, nesse caso, que G e J são *grupos isomorfos*. O isomorfismo f^{-1} é chamado *isomorfismo inverso* de f. Notação para grupos isomorfos: $G \simeq J$.

2) Se $x \longmapsto f(x)$ é um isomorfismo do grupo G no grupo J, muitas vezes não se faz distinção entre o grupo G e o grupo J, identificando cada $x \in G$ com $f(x) \in J$, de acordo com a idéia esboçada no início deste item.

* Mas isso não é geral: há grupos de ordem 4, por exemplo, que como veremos depois, não podem ser considerados "indistintos".

5. GRUPOS DE TRANSLAÇÕES

(EXEMPLO IMPORTANTE DE ISOMORFISMO)

Definição 7: Seja $(G, .)$ um grupo (aqui também a notação multiplicativa é apenas uma questão de simplicidade de linguagem). Para cada $a \in G$ a *translação* à esquerda definida por *a* é a aplicação

$$\delta_a: G \longrightarrow G \text{ dada por } \delta_a(x) = ax, \quad \forall\, x \in G$$

Seja T(G) o conjunto das translações à esquerda definidas em G.* Como $ax = ay \Longrightarrow x = y$, é claro que toda translação é uma aplicação injetora. Por outro lado, para todo $z \in G$, vale a igualdade $z = a(a^{-1}z)$, o que mostra que uma translação é necessariamente sobrejetora. Donde $T(G) \subset S(G)$ (conjunto das permutações sobre G).

Proposição 8: T(G) é um subgrupo de S(G).

Demonstração: Notemos primeiro que, para todo $a \in G$:

$$(\delta_{a^{-1}} \circ \delta_a)(x) = \delta_{a^{-1}}(ax) = a^{-1}(ax) = x$$

e $(\delta_a \circ \delta_{a^{-1}})(x) = x$, $\forall\, x \in G$ (mesma dedução). Isto significa que

$$(\delta_a)^{-1} = \delta_{a^{-1}} \quad , \quad \forall\, a \in G.$$

Por outro lado, $\forall\, a, b \in G$:

$$(\delta_a \circ \delta_b)(x) = \delta_a(bx) = a(bx) = (ab)x = \delta_{ab}(x), \quad \forall\, x \in G.$$

Logo $\delta_a \circ \delta_b = \delta_{ab}$. Daí

$$\delta_a \circ (\delta_b)^{-1} = \delta_a \circ \delta_{b^{-1}} = \delta_{ab^{-1}} \quad , \quad \forall\, a, b \in G$$

o que é suficiente para concluirmos que T(G) é um subgrupo de S(G).

O teorema a seguir nos fornece um exemplo importante de isomorfismo.

Teorema 1 (Cayley): Todo grupo G é isomorfo a T(G) mediante a aplicação $a \longmapsto \delta_a$, $\forall\, a \in G$.

Demonstração: Indiquemos por $f: G \longrightarrow T(G)$ a aplicação definida no enunciado. Logo $f(a) = \delta_a$, $\forall\, a \in G$.

I) $\forall\, a, b \in G$,

$f(a) = f(b) \Longrightarrow \delta_a = \delta_b \Longrightarrow \delta_a(x) = \delta_b(x)$, $\forall\, x \in G \Longrightarrow ax = bx$, $\forall\, x \in G$ $\Longrightarrow a = b$.

Logo f é injetora.

* Analogamente, se poderia definir translações à direita: $\gamma_a(x) = xa$, $x \in G$.

II) É imediato que f é sobrejetora.

III) $\forall\ a, b \in G,\ f(ab) = \delta_{ab} = \delta_a \circ \delta_b = f(a) \circ f(b)$. ■

Nota: O teorema acima significa que, dado um grupo G existe um grupo formado de aplicações que não se distingue de G, algebricamente falando. Este último constitui um "modelo" ou "realização concreta" de G.

Exemplo: Um grupo $G = \{e, a, b\}$, de ordem 3, obedece à seguinte tábua (ver exercício 10):

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Um modelo deste grupo, obtido através do teorema de Cayley, é formado pelas seguintes aplicações

$$\delta_e: \begin{cases} e \longmapsto ee = e \\ a \longmapsto ea = a \\ b \longmapsto eb = b \end{cases} \qquad \delta_a: \begin{cases} e \longmapsto ae = a \\ a \longmapsto aa = b \\ b \longmapsto ab = e \end{cases} \qquad \delta_b: \begin{cases} e \longmapsto be = b \\ a \longmapsto ba = e \\ b \longmapsto bb = a \end{cases}$$

que constituem o grupo $T(G) = \{\delta_e, \delta_a, \delta_b\}$ cuja tábua é

$\circ$	δ_e	δ_a	δ_b
δ_e	δ_e	δ_a	δ_b
δ_a	δ_a	δ_b	δ_e
δ_b	δ_b	δ_e	δ_a

Tal tábua foi obtida pela composição dos elementos de T(G) entre si. Vejamos como se fez para compor δ_a com δ_b.

$$(\delta_a \circ \delta_b)\ (e) = \delta_a(\delta_b(e)) = \delta_a(b) = e$$
$$(\delta_a \circ \delta_b)\ (a) = \delta_a(\delta_b(a)) = \delta_a(e) = a$$
$$(\delta_a \circ \delta_b)\ (b) = \delta_a(\delta_b(b)) = \delta_a(a) = b$$

Logo $\delta_a \circ \delta_b = \delta_e$. Recomendamos ao leitor a comparação da tábua de G com a de T(G).

6. PRODUTOS DIRETOS (EXTERNOS) DE GRUPOS: NOÇÕES

Consideremos dois grupos $(G, .)$ e $(J, .)$ (a razão da notação multiplicativa é a mesma de sempre). Indiquemos pelo símbolo 1 o elemento neutro, tanto o de G como o de J. Nessas condições o conjunto $G \times J$ é também um grupo multiplicativo, considerando sobre ele a seguinte lei de composição interna:

$$(a, b)\ (a', b') = (aa', bb')$$

$\forall\ a, a' \in G$ e $\forall\ b, b' \in J$. De fato.

A verificação da propriedade associativa é imediata. O par (1, 1) é o elemento neutro dessa lei. Dado $(a, b) \in G \times J$, como

$$(a, b)\ (a^{-1}, b^{-1}) = (a^{-1}, b^{-1})\ (a, b) = (1, 1)$$

então $(a, b)^{-1} = (a^{-1}, b^{-1})$.

Definição 8: O grupo $G \times J$ das considerações anteriores é chamado *produto direto* (externo) dos grupos G e J. *

Proposição 9: Consideremos o produto $G \times J$ de dois grupos G e J, conforme as considerações anteriores. Então:

a) $G \times \{1\} = \{(x, 1) \mid x \in G\}$ e $\{1\} \times J = \{(1, y) \mid y \in J\}$ são subgrupos de $G \times J$.

b) $G \simeq G \times \{1\}$ e $J \simeq \{1\} \times J$

Demonstração

a) Dados $(a, 1), (b, 1) \in G \times \{1\}$, temos

$$(a, 1)(b, 1)^{-1} = (a, 1)(b^{-1}, 1) = (ab^{-1}, 1) \in G \times \{1\}.$$

Logo $G \times \{1\}$ é subgrupo de $G \times J$. De maneira análoga se procede com relação a $\{1\} \times J$.

b) Seja $f: G \longrightarrow G \times \{1\}$ dada por $f(x) = (x, 1)$, $\forall\ x \in G$. Então:

(i) $f(xy) = (xy, 1) = (x, 1)(y, 1) = f(x)f(y)$, $\forall\ x, y \in G$

(ii) $N(f) = \{x \in G \mid (x, 1) = (1, 1)\}$. Logo $N(f) = \{1\}$ o que significa que f é injetora.

(iii) É evidente que f é sobrejetora: dado $(x, 1) \in G \times \{1\}$, então (x, 1) é imagem do elemento $x \in G$, mediante a aplicação f.

Que $J \simeq \{1\} \times J$ se verifica de modo semelhante. ■

Nota: A proposição anterior nos permite enxergar G e J como subgrupos de $G \times J$. Naturalmente "identificando" G com $G \times \{1\}$ e J com $\{1\} \times J$.

* Dados os grupos G e J, sempre que nos referirmos ao grupo $G \times J$, sem nenhuma outra menção, trata-se do produto direto aqui definido.

EXERCÍCIOS

36. Verificar em cada caso, se f é um homomorfismo

1º) $f: \mathbb{Z} \longrightarrow \mathbb{Z}$ dada por $f(x) = kx$, sendo $\mathbb{Z}$ o grupo aditivo dos inteiros e k um número inteiro dado.

2º) $f: \mathbb{R}^* \longrightarrow \mathbb{R}^*$ dada por $f(x) = |x|$, sendo $\mathbb{R}^*$ o grupo multiplicativo dos reais.

3º) $f: \mathbb{R} \longrightarrow \mathbb{R}$ dada por $f(x) = x + 1$, onde $\mathbb{R}$ é o grupo aditivo dos reais.

4º) $f: \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$; dada por $f(x) = (x, 0)$, onde $\mathbb{Z}$ e $\mathbb{Z} \times \mathbb{Z}$ denotam grupos aditivos.

5º) $f: \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$, dada por $f(x, y) = x$, onde $\mathbb{Z}$ e $\mathbb{Z} \times \mathbb{Z}$ são grupos aditivos.

6º) $f: \mathbb{Z} \longrightarrow \mathbb{R}_+^*$, dada por $f(x) = 2^x$, onde $\mathbb{Z}$ é grupo aditivo e $\mathbb{R}_+^*$ é grupo multiplicativo.

37. Determinar os homomorfismos injetores e os sobrejetores do exercício anterior.

38. Determinar o núcleo em cada homomorfismo do exercício 36.

39. Seja $f: \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ definida por $f(x, y) = (x - y, 0)$. Provar que f é um homomorfismo do grupo aditivo $\mathbb{Z} \times \mathbb{Z}$ em si próprio. Obter N(f).

40. Das aplicações abaixo algumas são endomorfismos do grupo multiplicativo dos complexos. Descubra quais e determine o núcleo destas:

I) $z \longmapsto z^2$

II) $z \longmapsto |z|$

III) $z \longmapsto \overline{z}$

IV) $z \longmapsto \frac{1}{z}$

V) $z \longmapsto -\frac{1}{z}$

VI) $z \longmapsto -z$

VII) $z \longmapsto z^3$.

41. Dado o homomorfismo $f: \mathbb{Z} \longrightarrow \mathbb{C}^*$ dado por $f(m) = i^m$, $\forall\, m \in \mathbb{Z}$, ache $f(2\mathbb{Z})$ e $f(3\mathbb{Z})$.

42. Sejam G e J grupos multiplicativos, f é um homomorfismo de G em J e H um subgrupo de J. Mostre que $f^{-1}(H) = \{x \in G \mid f(x) \in H\}$ é um subgrupo de G. Considerando o homomorfismo do exercício anterior o que é $f^{-1}(\{1, -1\})$?

43. Sejam G um grupo multiplicativo comutativo e n um número inteiro positivo. Mostrar que a aplicação $f(x) = x^n$ é um homomorfismo de G em si mesmo.

Definição: $x^0 = e$ (elemento neutro) e $x^n = x.x.\ldots.x$ (n fatores).

44. Prove que um grupo G é abeliano se, e somente se, $f: G \longrightarrow G$ definida por $f(x) = x^{-1}$ é um homomorfismo.

45. A aplicação $f = \{(\overline{0}, e), (\overline{1}, a), (\overline{2}, b), (\overline{3}, c)\}$ é um isomorfismo do grupo $(\mathbb{Z}_4, +)$ no grupo (G, ·). Construir a tábua de G; calcular a^2 e b^{-3}; determinar $x \in G$ tal que $axb^2 = c^3$.

Solução 1

Construímos a tábua de $(\mathbb{Z}_4, +)$ e, em seguida, fazemos a tábua de (G, ·) substituindo cada elemento de $\mathbb{Z}_4$ pela sua imagem no isomorfismo f.

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

·	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$a^2 = a \cdot a = b$

$b^{-3} = (b^{-1})^3 = b^3 = b^2 \cdot b = e \cdot b = b$

Solução 2

1º) $e = f(0)$ é o elemento neutro de G, portanto, $e \cdot x = x = x \cdot e$, $\forall\, x \in G$.

2º) Devido à propriedade $f(-x) = (f(x))^{-1}$. Temos:

$a^{-1} = (f(\overline{1}))^{-1} = f(-\overline{1}) = f(\overline{3}) = c$

e também $b^{-1} = b$ e $c^{-1} = a$.

3º) Como todo elemento de G é regular e distinto dos outros três, vem:

$a \cdot b = b \cdot a = c$, $b \cdot c = c \cdot b = a$, $a \cdot a = c$ e $c \cdot c = b$.

46. Construir a tábua de um grupo $G = \{e, a, b, c\}$ que seja isomorfo ao grupo multiplicativo $H = \{1, -1, i, -i\}$.

47. Prove que o grupo $G_1 = \mathcal{P}(\{a, b\})$ com a operação diferença simétrica e o grupo $G_2 = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ com a operação de multiplicação módulo 8 são isomorfos.

48. Mostre que o grupo de Klein e o grupo cíclico de ordem 4 não são isomorfos.

Sugestão: Tomar um homomorfismo f e mostrar que f não é bijetora.

49. Mostre que para um grupo com 4 elementos é possível construir duas, e apenas duas, tábuas distintas.

Sugestão: $G = \{e, a, b, c\}$ e notar que $a * b = e$ ou c.

50. Sabendo que $G = \{e, a, b, c, d, f\}$ é um grupo multiplicativo isomorfo do grupo $(\mathbb{Z}_6, +)$, pede-se:

a) construir uma tábua para G;

b) calcular a^2, b^{-2} e c^{-3};

c) obter $x \in G$ tal que $dxf = a^{-1}$.

51. Mostre que $f: \mathbb{Z} \longrightarrow 2\mathbb{Z} = \{0, \pm 2, \pm 4, \ldots\}$ dada por $f(m) = 2m$, $\forall\, m \in \mathbb{Z}$, é um isomorfismo de $(\mathbb{Z}, +)$ em $(2\mathbb{Z}, +)$.

52. I) Seja $a \in \mathbb{R}_+^*$, $a \neq 1$. Mostre que $G = \{a^n \mid n \in \mathbb{Z}\}$ é um subgrupo de $(\mathbb{R}_+^*, \cdot)$.
II) Mostre que $n \longrightarrow a^n$ define um isomorfismo de $(\mathbb{Z}, +)$ em $(G, \cdot)$.

53. Provar que a função exponencial $f(x) = a^x$; com $0 < a \neq 1$, é um isomorfismo do grupo aditivo $\mathbb{R}$ no grupo multiplicativo $\mathbb{R}_+^*$. Qual é o isomorfismo inverso?

54. Mostre $G = \{2^m 3^n \mid m, n \in \mathbb{Z}\}$ e $J = \{m + ni \mid m, n \in \mathbb{Z}\}$ são subgrupos de $(\mathbb{R}_+^*, \cdot)$ e de $(\mathbb{C}, +)$, respectivamente, e que são isomorfos.

55. Determinar todos os automorfismos do grupo de Klein.

56. Indicando com Aut(G) o conjunto de todos os automorfismos de um grupo G, mostrar que $(\text{Aut}(G), \circ)$ é um grupo.

57. Mostre que h é um automorfismo do grupo aditivo dos racionais se, e somente se, $\exists\ c \in \mathbb{Q}^*$ de forma que $h(x) = cx$, $\forall\ x \in \mathbb{Q}$.

58. Seja a um elemento fixo do grupo G. Prove que $f : G \longrightarrow G$ definida por $f(x) = axa^{-1}$ é um isomorfismo.

59. Mostre que há pelo menos dois endomorfismo em cada grupo e ao menos um isomorfismo.

60. Dados os grupos $(G, \cdot)$ e $(J, \cdot)$ considere o produto direto de G por J. Quais das seguintes aplicações são homomorfismos? Destas ache o núcleo.
I) $(x, y) \longmapsto x$, de GxJ em G
II) $(x, y) \longmapsto y$, de GxJ em J
III) $x \longmapsto (x, 1)$ de G em GxJ
IV) $(x, y) \longmapsto (y, x)$ de GxJ em JxG
V) $y \longmapsto (1, y)$ de J em GxJ.

§ 3º — GRUPOS CÍCLICOS
GRUPOS GERADOS POR UM SUBCONJUNTO

1. POTÊNCIAS E MÚLTIPLOS

Definição 9: Seja G um grupo multiplicativo. Dado $a \in G$, define-se *potência* m-ésima de a, para todo inteiro m, da seguinte maneira:

se $m \geq 0$, por recorrência da seguinte forma

$a^0 = e$ (elemento neutro de G),

$a^m = a^{m-1}a$, se $m \geq 1$;

se $m < 0$, por

$a^m = (a^{-m})^{-1}$.

1º) No grupo multiplicativo $GL_2(\mathbb{R})$, tomando o elemento $a = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}$ temos:

$$a^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$a^2 = a \cdot a = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 8 & 11 \end{pmatrix}$$

$$a^{-1} = \left(\frac{1}{\det a}\right)\text{adj}(a)$$

$$a^{-2} = (a^2)^{-1} = \begin{pmatrix} 3 & 4 \\ 8 & 11 \end{pmatrix}^{-1} = \frac{1}{33-32} \cdot \begin{pmatrix} 11 & -4 \\ -8 & 3 \end{pmatrix} = \begin{pmatrix} 11 & -4 \\ -8 & 3 \end{pmatrix}$$

2º) No grupo multiplicativo $\mathbb{Z}_5^*$, tomando o elemento $\bar{2}$, temos:

$\bar{2}^0 = \bar{1}$, $\bar{2}^2 = \bar{2} \cdot \bar{2} = \bar{4}$, $\bar{2}^3 = \bar{2} \cdot \bar{2} \cdot \bar{2} = \bar{3}$,

$(\bar{2})^{-1} = \bar{3}$, $(\bar{2})^{-2} = (\bar{2}^2)^{-1} = (\bar{4})^{-1} = \bar{4}$, etc.

3º) Dada a permutação $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, temos, segundo a definição:

$$a^0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \text{elemento neutro de } S_3,$$

$$a^2 = a \circ a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$a^3 = a^2 \circ a = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},$$

$$a^{-2} = (a^2)^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \text{ etc.}$$

Da definição dada decorrem as seguintes propriedades:

a) $a^m a^n = a^{m+n}$, $\forall\ a \in G$ e $\forall\ m, n \in \mathbb{Z}$;

b) $(a^m)^n = a^{mn}$, $\forall\ a \in G$ e $\forall\ m, n \in \mathbb{Z}$;

c) $a^{-m} = (a^m)^{-1} = (a^{-1})^m$, $\forall\ a \in G$ e $\forall\ m \in \mathbb{Z}$

Provaremos a seguir a primeira dessas propriedades. As outras deixamos como exercício.

Proposição 10: Dado um grupo multiplicativo G, se $a \in G$ e $m, n \in \mathbb{Z}$, então $a^m a^n = a^{m+n}$.

Demonstração:

(I) $n \geqslant 0$ e $m + n \geqslant 0$. (Este caso será tratado por indução sobre n).

$n = 0 \Longrightarrow a^m a^n = a^m a^0 = a^m e = a^m = a^{m+0} = a^{m+n}$

Suponhamos $a^m a^r = a^{m+r}$, onde $r \geqslant 0$. Daí

$a^m a^{r+1} = a^m (a^r a) = (a^m a^r) a = a^{m+r} a = a^{(m+r)+1} = a^{m+(r+1)}$

(II) Suponhamos agora que m e n são dois inteiros quaisquer. Tomemos um número inteiro $p > 0$ tal que $p + m > 0$, $p + n > 0$ e $p + m + n > 0$. Então, observando que $a^p a^{-p} = a^p (a^p)^{-1} = e$ (como conseqüência da definição) temos:

$a^{m+n} = a^{m+n}(a^p a^{-p}) = (a^{m+n} a^p) a^{-p} \overset{*}{=} a^{(m+n)+p} a^{-p} = a^{m+(n+p)} a^{-p} \overset{*}{=}$

$= (a^m (a^n a^p)) a^{-p} = ((a^m a^n) a^p) a^{-p} = (a^m a^n)(a^p a^{-p}) = (a^m a^n) e = a^m a^n$. ■

Nota: Para um grupo aditivo G define-se *múltiplo* (ao invés de potência) de um elemento $a \in G$ da seguinte maneira:

a) $m \geqslant 0$, por recorrência assim

$0a = e$ (elemento neutro de G) e $ma = (m-1)a + a$, se $m \geqslant 1$;

b) se $m < 0$, então $ma = (-m)(-a)$.

* Usando a primeira parte da demonstração.

Exemplo: No grupo aditivo $\mathbb{Z}_4$, tomando o elemento $\bar{3}$, temos:

$0 \cdot \bar{3} = \bar{0}$, $2 \cdot \bar{3} = \bar{3} + \bar{3} = \bar{2}$, $3 \cdot \bar{3} = \bar{3} + \bar{3} + \bar{3} = \bar{1}$, $-\bar{3} = \bar{1}$, $-2 \cdot \bar{3} = -(2 \cdot \bar{3}) = -\bar{2} = \bar{2}$, etc.

O elemento ma é chamado múltiplo de a segundo m. É claro que nessa definição $m \in \mathbb{Z}$. As propriedades, paralelas às que enunciamos para potências, são as seguintes:

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

b) $m(na) = (mn)a$

c) $(-m)a = m(-a) = -(ma)$, $\forall\ m, n \in \mathbb{Z}$ e $\forall\ a \in G$

2. GRUPOS CÍCLICOS

Definição 10: Um grupo multiplicativo G se denomina *grupo cíclico* se existe um elemento $a \in G$ de maneira que $G = \{a^m \mid m \in \mathbb{Z}\}$. Notação $G = [a]$. O elemento a é dito *gerador* de G.

Exemplos:

1) O grupo multiplicativo $G = \{1, -1\}$ é cíclico uma vez que $\{(-1)^m \mid m \in \mathbb{Z}\} = \{1, -1\} = G$

2) O grupo multiplicativo dos números racionais não é cíclico. É claro que não existe um número racional $\frac{r}{s} \neq 0$ do qual todos os números racionais não nulos sejam potências, pois isto acarretaria que o conjunto dos números primos é finito, o que é absurdo. Sugerimos ao leitor tentar justificar com detalhes a explicação dada. Para tanto deverá usar o teorema fundamental da aritmética.

Notas:

a) Todo grupo cíclico é abeliano pois $a^m a^n = a^{m+n} = a^{n+m} = a^n a^m$.

b) Um mesmo grupo cíclico pode conter mais do que um gerador. Ver exercício 78.

c) Se G é um grupo aditivo cíclico gerado por a, então $G = \{ma \mid m \in \mathbb{Z}\} = [a]$.

Proposição 11: Dado um grupo multiplicativo G, se $a \in G$, então o subconjunto $H = \{a^m \mid m \in \mathbb{Z}\}$ é um subgrupo de G.

Demonstração: Como $a^0 = e$, então $e \in H$. Por outro lado, se $x, y \in H$, então existem $m, n \in \mathbb{Z}$ de maneira que $x = a^m$ e $y = a^n$. Daí

$$xy^{-1} = a^m a^{-n} = a^{m-n} \in H. \quad ■$$

A proposição anterior nos diz que todo elemento a de um grupo G é gerador de um subgrupo cíclico. Tal subgrupo será indicado por [a] notação que é coerente com a da definição 10. Assim: $[a] = \{a^m \mid m \in \mathbb{Z}\}$.

Exemplos:

I) No grupo multiplicativo dos complexos: $[i] = \{1, -1, i, -i\}$

II) No grupo multiplicativo dos reais: $[-1] = \{1, -1\}$

III) No grupo multiplicativo dos racionais: $[2] = \{\ldots, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, \ldots\}$

IV) No grupo aditivo dos inteiros: $[1]_+ = [-1]_+ = \mathbb{Z}$ o que significa que $\mathbb{Z}$ é cíclico.

V) No grupo S_3 se $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $[a] = \{\text{el. neutro}, a\}$. Recomendamos ao leitor os cálculos neste caso.

3. GRUPOS CÍCLICOS INFINITOS

Seja G um grupo multiplicativo cujo elemento neutro indicaremos por e. Suponhamos que a seja um elemento de G com a seguinte característica:

$$a^m = e \iff m = 0$$

O elemento 2 no grupo multiplicativo dos reais tem nessa propriedade já que

$$2^m = 1 \iff m = 0.$$

Nesse caso vale a seguinte proposição:

Proposição 12: A aplicação $f: \mathbb{Z} \longrightarrow [a]$, dada por $f(m) = a^m$, $\forall\ m \in \mathbb{Z}$, é um isomorfismo do grupo aditivo $\mathbb{Z}$ no grupo $[a]$.

Demonstração: (i) $f(m+n) = a^{m+n} = a^m a^n = f(m)f(n)$, $\forall\ m, n \in \mathbb{Z}$; (ii) $N(f) = \{m \in \mathbb{Z} \mid a^m = e\} = \{0\}$, devido à hipótese subjacente ao caso que estamos considerando; (iii) é óbvio que f é sobrejetora: todo $a^r \in [a]$ provém de r através de f. ■

Definição 11: Dado um elemento a de um grupo multiplicativo G, se

$$a^m = e \iff m = 0$$

dizemos que o elemento a tem *período zero* (*) e que o grupo $[\ a\ ]$ é um *grupo cíclico infinito*.

Exemplo: O elemento 2 tem período zero no grupo multiplicativo dos reais, conforme já vimos. O isomorfismo entre $\mathbb{Z}$ e $[2]$ pode ser assim visualizado:

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$
$$\downarrow\ \downarrow\ \downarrow\ \downarrow\ \downarrow$$
$$[\ 2\ ] = \{\ldots, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, \ldots\}$$

* ou *ordem* zero.

4. GRUPOS CÍCLICOS FINITOS

Consideremos agora a possibilidade contrária à considerada no item anterior: a é um elemento de um grupo multiplicativo G e

$\exists\ m \in \mathbb{Z}$, $m \neq 0$, de modo que $a^m = e$ (el. neutro de G).

Neste caso

$$a^{-m} = (a^m)^{-1} = e^{-1} = e.$$

Logo podemos dizer que, com a hipótese considerada agora, existe um número inteiro $r > 0$, de maneira que $a^r = e$.

Definição 12: O menor número inteiro $h > 0$ tal que $a^h = e$ chama-se *período* ou *ordem* do elemento a. Notação: $o(a) = h$.

Exemplos:

(i) O elemento $i \in \mathbb{C}^*$ tem período 4 porque
$i^1 = i$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$.

(ii) O período do elemento (-1) no grupo multiplicativo $\mathbb{Q}^*$ é 2 pois
$(-1)^1 = -1$, $(-1)^2 = 1$.

(iii) O período do elemento $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ no grupo S_3 é 2. A razão é a seguinte:

$$a^1 = a,\ a^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \text{el. neutro}$$

Proposição 13: Seja a um elemento de um grupo multiplicativo G. Se a ordem de a é $h > 0$, então $[\ a\ ]$ é um grupo finito de ordem h dado por $[\ a\ ] = \{e, a, a^2, \ldots, a^{h-1}\}$.

Demonstração: Mostremos primeiro que o conjunto $\{e, a, \ldots, a^{h-1}\}$ tem exatamente h elementos. De fato:

$0 \leqslant i < j < h$ e $a^i = a^j \Rightarrow 0 < j - i < h$ e $a^{j-i} = e$ (absurdo pois $o(a) = h$). Logo não há elementos iguais nesse conjunto e são h os seus elementos.

Mostremos agora que $[a] = \{e, a, a^2, \ldots, a^{h-1}\}$ para o que é suficiente mostrar que o primeiro desses conjuntos está contido no segundo. Ora, $\forall\ x \in [a]$, existe $m \in \mathbb{Z}$ de maneira que $x = a^m$. Usando o algorítmo da divisão em $\mathbb{Z}$ com relação aos elementos m e h temos

$$\exists\ q, r \in \mathbb{Z} \mid m = hq + r \quad (0 \leqslant r < h).$$

Daí:

$$x = a^m = a^{hq+r} = a^{hq}a^r = (a^h)^q a^r = e^q a^r = ea^r = a^r.$$

Como $0 \leqslant r < h$, então $x \in \{e, a, a^2, \ldots, a^{h-1}\}$. ■

A proposição que acabamos de provar acarreta que, se o período de um elemento a de um grupo G é $h > 0$, então a ordem do subgrupo gerado por a também é h: $o(a) = o([a])$. A definição a seguir é propiciada pela proposição 13.

Definição 13: Seja $G = [a]$ um grupo cíclico. Dizemos que G é um *grupo cíclico finito* se o período do elemento a for um número natural $h > 0$. Pelo que já vimos é claro que neste caso $G = \{e, a, a^2, \ldots, a^{h-1}\}$.

Proposição 14: Seja a um elemento de período $h > 0$ de um grupo G. Então: $a^m = e \iff h \mid m$.

Demonstração: ($\Longrightarrow$) Dado $m \in \mathbb{Z}$, existem $q, r \in \mathbb{Z}$ de maneira que $m = hq + r \quad (0 \leqslant r < h)$. Daí:

$$e = a^m = a^{hq+r} = (a^h)^q a^r = e^q a^r = ea^r = a^r.$$

Como $r < h$, então $r = 0$ (pois o período de a é h). Assim, $m = hq$ e $h \mid m$.

($\Longleftarrow$) Se $h \mid m$, então existe $q \in \mathbb{Z}$ de maneira que $m = hq$. Donde

$$a^m = a^{hq} = (a^h)^q = e^q = e. \quad \blacksquare$$

Proposição 15: Seja G um grupo cíclico finito de ordem h. Então G é isomorfo ao grupo aditivo $\mathbb{Z}_h$.

Demonstração: Se a é gerador de G, então $G = \{e, a, a^2, \ldots, a^{h-1}\}$. Consideremos a correspondência $\bar{s} \longmapsto a^s$ de $\mathbb{Z}_h$ em G. Trata-se de uma aplicação injetora porque

$$\bar{s} = \bar{t} \iff s \equiv t \pmod h \iff (\exists\, q \in \mathbb{Z} \mid s - t = hq) \iff a^{s-t} = a^{hq} = e \iff a^s = a^t$$

É claro que é uma aplicação sobrejetora. Para mostrar que é um homomorfismo vamos dar o nome a ela de f. Então

$$f(\bar{s} + \bar{t}) = f(\overline{s+t}) = a^{s+t} = a^s a^t = f(\bar{s})f(\bar{t}),\ \forall\ \bar{s}, \bar{t} \in \mathbb{Z}_h. \quad \blacksquare$$

Esta proposição significa que quando tivermos de pensar em grupos cíclicos finitos podemos pensar em grupos aditivos de classes de restos.

5. GRUPOS GERADOS POR SUBCONJUNTOS (NOÇÕES)

A noção de grupo cíclico pode ser generalizada. É o que veremos neste item.

Seja G um grupo multiplicativo. Dado um subconjunto não vazio $L \subset G$, Vamos construir, a partir de L, um outro subconjunto de G o qual indicaremos por [L]. É o seguinte

$$[L] = \{a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_t^{\alpha_t} \mid t \geqslant 1,\ a_1, \ldots, a_t \in L \text{ e } \alpha_1, \ldots, \alpha_t \in \mathbb{Z}\}$$

Obviamente $[L] \neq \phi$ pois, inclusive, $L \subset [L]$ (verifique). Mostraremos que [L] é um subgrupo de G. De fato, dados $x, y \in [L]$, então

$x = a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_t^{\alpha_t}$ e $y = b_1^{\beta_1} b_2^{\beta_2} \ldots b_s^{\beta_s}$, onde $a_i, b_j \in L$ e $\alpha_i, \beta_j \in \mathbb{Z}$.

Daí

$$xy^{-1} = a_1^{\alpha_1} \ldots a_t^{\alpha_t} b_s^{-\beta_s} \ldots b_1^{-\beta_1}$$

o que significa que $xy^{-1} \in [L]$.

Logo [L] é um subgrupo de G. É o "menor" subgrupo de G que contém L, isto é, dado um subgrupo K de G, se $L \subset K$, então $[L] \subset K$. Deixamos como exercício a verificação dessa afirmativa. É claro, por outro lado, que se $L = \{a\}$, então $[L] = \{a^m \mid m \in \mathbb{Z}\}$ é o subgrupo cíclico gerado por a.

Definição 14: O grupo [L] obtido por intermédio das considerações anteriores é chamado *subgrupo gerado* por L. Quando existe um subconjunto finito e não vazio L de modo que $[L] = G$, dizemos que o grupo G é um *grupo de tipo finito.*

Exemplos:

1) Todo grupo cíclico é de tipo finito.

2) O produto direto de dois grupos cíclicos $G = [a]$ e $K = [b]$ é de tipo finito porque tomando $L = \{(a, 1), (1, b)\} \subset G \times K$, então $[L] = G \times K$ pois, $\forall\ (a^r, a^s) \in G \times K$,

$$(a^r, a^s) = (a, 1)^r (1, b)^s.$$

3) Um grupo diedral $D_{2n} = \{e, a, \ldots, a^{n-1}, b, ba, \ldots, ba^{n-1}\}$ é gerado por $L = \{a, b\}$.

EXERCÍCIOS

61. Construa os seguintes subgrupos:
   a) $[-1]_+$ em $(\mathbb{Q}, +)$
   b) $[3]_+$ em $(\mathbb{Z}, +)$
   c) $[3]$ em $(\mathbb{Q}^*, \cdot)$
   d) $[i]$ em $(\mathbb{C}^*, \cdot)$

62. Mostre que todo grupo de ordem 2 ou 3 é cíclico.

63. Ache um grupo de ordem 4 cíclico e um não cíclico.

64. Mostre que $(\mathbb{Z}_m, +)$ é cíclico, $\forall\ m > 1$.

65. Mostre que todo grupo cíclico infinito tem dois e somente dois geradores.

66. Mostre que todo subgrupo $H \neq \{e\}$ de um grupo cíclico infinito é também infinito.

67. A tábua ao lado define uma operação $\cdot$ que confere ao conjunto $E = \{e, a, b, c, d, f\}$ uma estrutura de grupo.

$\cdot$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	c	d	f	e
b	b	c	d	f	e	a
c	c	d	f	e	a	b
d	d	f	e	a	b	c
f	f	e	a	b	c	d

Pede-se determinar:

1º) o subgrupo gerado por b;

2º) o período de d;

3º) os geradores de G;

4º) $x \in G$ tal que $bxc = d^{-1}$.

Solução

1º) $b^0 = e,\ b^1 = b,\ b^2 = d,\ b^3 = b^2b = db = e$

$[b] = \{e, b, d\}$

2º) $d^0 = e,\ d^1 = d,\ d^2 = b,\ d^3 = e$

então $o(d) = 3$

3º) Já sabemos que e, b, d não são geradores de G. Por outro lado:

$[a] = \{e, a, b, c, d, f\} = [f]$

$[c] = \{e, c\}$

portanto, os geradores de G são a e f

4º) $bxc = d^{-1} \iff b^{-1}bxcc^{-1} = b^{-1}d^{-1}c^{-1} \iff x = b^{-1}d^{-1}c^{-1}$ então

$x = dbc = ec = c$

68. Seja $G = \{e, a, b, c, d, f, g, h\}$ um grupo cuja tábua está abaixo. Pede-se determinar:

$\cdot$	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	d	c	g	f	e	h	b
b	b	h	d	a	g	c	e	f
c	c	b	f	d	h	g	a	e
d	d	f	g	h	e	a	b	c
f	f	e	h	b	a	d	c	g
g	g	c	e	f	b	h	d	a
h	h	g	a	e	c	b	f	d

1º) o subgrupo gerado por b;

2º) o período de d;

3º) Os geradores de G;

4º) $x \in G$ tal que $a \cdot x \cdot b^{-1} = d$.

69. Sejam $m \in \mathbb{Z}$, $m > 1$. Indicando por G_m o conjunto das raízes m-ésimas complexas de 1, mostre que $(G_m, \cdot)$ é um subgrupo cíclico de $(\mathbb{C}^*, \cdot)$.

70. Mostre que o único elemento de um grupo de período um é o elemento neutro.

71. Seja $a \neq e$ um elemento do grupo G. Prove que $o(a) = 2$ se, e somente se, $a = a^{-1}$.

72. Seja G um grupo finito de ordem par. Mostre que o número de elemento de G de período 2 é ímpar.

73. Sejam G um grupo multiplicativo e $x \in G$. Mostrar que se existe um inteiro n, $n \geq 1$, tal que $x^n = e$, então existe um inteiro $m \geq 1$ tal que $x^{-1} = x^m$.

74. Sejam a e b elementos de um grupo multiplicativo G. Supondo $o(ab) = h > 0$, mostre que $o(ba) = h$.

Solução

Se $o(a, b) = h > 0$, temos:

$(ab)^h = e$ e $(ab)^i \neq e, \qquad i \in \{1, 2, \ldots, h-1\}$

Temos, por outro lado:

1º) $(ba)^h = b(ab)^{h-1}a = b(ab)^{-1}a = bb^{-1}a^{-1}a = e$

2º) Se $i \in \{1, 2, \ldots, h-1\}$ e $(ba)^i = e$, decorre:

$b(ab)^{i-1}a = e \ \therefore (ab)^{i-1} = b^{-1}a^{-1} \ \therefore (ab)^{i-1} = (ab)^{-1}$

isto é, $(ab)^i = e$ e isto é absurdo.

75. Se a, b e ab do grupo multiplicativo G têm período 2, então $ab = ba$. Prove.

76. Seja G um grupo multiplicativo e suponha $a \in G$. Mostre que $o(a) = o(a^{-1}) = o(xax^{-1})$, $\forall\, x \in G$.

77. Seja G um grupo finito. Se $x \in G$, mostre que $\exists\ n \in \mathbb{Z}$ de modo que $x^n = e$ (elemento neutro).

78. Seja $G = [a]$ um grupo cíclico de ordem h. Mostre que:

$a^t \in G$ é um gerador de $G \iff \text{mdc}(h, t) = 1$.

Solução

$(\Longrightarrow)$

Se a^t é um gerador de G, como $a \in G$, temos:

$\exists\ r \in \mathbb{N} \mid (a^t)^r = a \ \therefore a^{tr} = a \ \therefore tr \equiv 1 \pmod{h} \ \therefore tr = 1 + kh \ \therefore 1 = tr - kh$

Seja $d = \text{mdc}(h, t)$. Então:

$$\left.\begin{array}{l} d \mid t \implies d \mid tr \\ d \mid h \implies d \mid kh \end{array}\right\} \implies d \mid tr - kh \implies d \mid 1 \implies d = 1$$

($\Longleftarrow$)

Se $1 = \text{mdc}(h, t)$, então existem dois inteiros r e s tais que $1 = rt + hs$ e, daí, $rt \equiv 1 \pmod{h}$, portanto, $a^{rt} = a$.

Dado $x \in G$, temos:

$x = a^i = (a^{rt})^i = (a^t)^{ri}$

o que prova que a^t é gerador de G.

79. Mostre que todo subgrupo de um grupo cíclico é, também cíclico.

80. Se $G = [a]$ é um grupo cíclico de ordem $h > 0$ e se d é um divisor positivo de h, mostre que, sendo $t = h : d$, então $[a^t]$ é um subgrupo cíclico de G de ordem d.

81. A) Defina subgrupo gerado por um subconjunto de elementos de um grupo aditivo.

B) Mostre que $(\mathbb{Z}^n, +)$ é de tipo finito, $\forall n \geqslant 1$.

82. Mostre que $(\mathbb{Q}, +)$ não é de tipo finito.

83. Seja S uma parte não vazia de um grupo multiplicativo G. Mostre que todo subgrupo de G que contém S também contém [S].

§ 4º — CLASSES LATERAIS — TEOREMA DE LAGRANGE

1. CLASSES LATERAIS

Definição 15: Seja H um subgrupo de um grupo $(G, *)$. Dado $a \in G$ indicaremos por $a * H$ (respectivamente por $H * a$) e chamaremos de *classe lateral* à esquerda (respectivamente à direita), módulo H, definida por a, o seguinte subconjunto de G:

$$a * H = \{a * x \mid x \in H\}$$

(respectivamente, $H * a = \{x * a \mid x \in H\}$). Se G é um grupo comutativo é claro que $a * H = H * a$, $\forall\ a \in G$.

Exemplos:

1º) Sejam o grupo multiplicativo $G = \{1, i, -1, -i\}$ e seu subgrupo $H = \{1, -1\}$. Temos:

$1 \cdot H = \{1 \cdot 1, 1 \cdot (-1)\} = \{1, -1\} = H \cdot 1$

$(-1) \cdot H = \{(-1) \cdot 1, (-1) \cdot (-1)\} = \{-1, 1\} = H \cdot (-1)$

$i \cdot H = \{i \cdot 1, i \cdot (-1)\} = \{i, -i\} = H \cdot i$

$(-i) \cdot H = \{(-i) \cdot 1, (-i) \cdot (-1)\} = \{-i, i\} = H \cdot (-i)$

2º) Sejam o grupo aditivo $G = Z_6$ e seu subgrupo $H = \{\bar{0}, \bar{3}\}$. Temos:

$\bar{0} + H = \{\bar{0} + \bar{0}, \bar{0} + \bar{3}\} = \{\bar{0}, \bar{3}\} = H + \bar{0}$

$\bar{1} + H = \{\bar{1} + \bar{0}, \bar{1} + \bar{3}\} = \{\bar{1}, \bar{4}\} = H + \bar{1}$

$\bar{2} + H = \{\bar{2} + \bar{0}, \bar{2} + \bar{3}\} = \{\bar{2}, \bar{5}\} = H + \bar{2}$

$\bar{3} + H = \{\bar{3} + \bar{0}, \bar{3} + \bar{3}\} = \{\bar{3}, \bar{0}\} = H + \bar{3}$

$\bar{4} + H = \{\bar{4} + \bar{0}, \bar{4} + \bar{3}\} = \{\bar{4}, \bar{1}\} = H + \bar{4}$

$\bar{5} + H = \{\bar{5} + \bar{0}, \bar{5} + \bar{3}\} = \{\bar{5}, \bar{2}\} = H + \bar{5}$

3º) Sejam G o grupo multiplicativo dos reais e $H = \{x \in \mathbb{R}^* \mid x > 0\}$. Então,

$\forall\ a > 0 \Longrightarrow aH = H$

$\forall\ a < 0 \Longrightarrow aH = \{x \in \mathbb{R}^* \mid x < 0\}$.

4º) Consideremos o grupo diedral $D_6 = \{e, a, a^2, b, ba, ba^2\}$ cuja tábua se encontra no exemplo (m), item 4, § 1, deste capítulo. O subconjunto $H = \{e, b\}$ é um subgrupo de D_6 (verifique). Determinemos as classes laterais, à esquerda e à direita, módulo H.

$eH = \{e, b\}$	$He = \{e, b\}$
$aH = \{a, ba^2\}$	$Ha = \{a, ba\}$
$a^2H = \{a^2, ba\}$	$Ha^2 = \{a^2, ba^2\}$
$bH = \{b, e\}$	$Hb = \{b, e\}$
$(ba)H = \{ba, a^2\}$	$H(ba) = \{ba, a\}$
$(ba^2)H = \{ba^2, a\}$	$H(ba^2) = \{ba^2, a^2\}$

Observemos que, neste exemplo, $aH \neq Ha$, $a^2H \neq Ha^2$, $(ba)H \neq H(ba)$ e $(ba^2)H \neq H(ba^2)$

2. PROPOSIÇÕES SOBRE CLASSES LATERAIS

Nas considerações abaixo usaremos novamente a notação multiplicativa para indicar a lei de composição de um grupo arbitrário. A razão dessa escolha é a mesma de sempre. Trabalharemos, ademais, com classes laterais à esquerda, uma vez que para o que temos em vista tanto faz usar classes à direita ou à esquerda. Inclusive as demonstrações seriam análogas com classes à direita. Seja pois G um grupo multiplicativo e suponhamos H um subgrupo de G. .

Proposição 16: A união de todas as classes laterais módulo H é igual a G.

Demonstração: Seja e o elemento neutro de G. Então $e \in H$. Logo todo elemento $a \in G$ pertence à classe aH pois $a = ae$. Se cada elemento de G está numa classe lateral à esquerda, módulo H, nossa afirmação está provado. ■

Proposição 17: $(\forall\ a, b \in G)(aH = bH \iff a^{-1}b \in H)$.

Demonstração: ($\Longrightarrow$) Vimos na demonstração anterior que $a \in aH$. Como $aH = bH$, então $a \in bH$. Daí existe $h \in H$ de modo que $a = bh$. Donde $a^{-1}b = h^{-1} \in H$.

($\Longleftarrow$) Como $a^{-1}b \in H$, então existe $h \in H$ tal que $a^{-1}b = h$. Disto resulta que $a = bh^{-1}$.

Seja $y \in aH$. Então $y = ah_1$, onde h_1 é um elemento conveniente de H. Donde

$$y = ah_1 = (bh^{-1})h_1 = b(h^{-1}h_1)$$

o que vem mostrar que $y \in bH$. Assim provamos que $aH \subset bH$. É claro que também $bH \subset aH$. Portanto, $aH = bH$. ■

Proposição 18: Sejam aH e bH duas classes laterais módulo H genéricas. Então $aH \cap bH = \phi$ ou $aH = bH$.

Demonstração: Suponhamos que exista $x \in aH \cap bH$. Então existem $h_1, h_2 \in H$ de forma que $x = ah_1 = bh_2$. Disto segue que $a^{-1}b = h_1h_2^{-1} \in H$. Pela proposição anterior podemos dizer que $aH = bH$. ■

Proposição 19: Toda classe lateral aH é equipotente a H.

Demonstração: A aplicação $f: H \longrightarrow aH$ dada por $f(h) = ah$, $\forall\ h \in H$, é uma bijeção pois (i) $f(h_1) = f(h_2) \Longrightarrow ah_1 = ah_2 \Longrightarrow h_1 = h_2$ e (ii) dado $ah \in aH$ é evidente que ah é a imagem de h pela aplicação f. ■

Nota: Das proposições acima podemos inferir que o conjunto das classes laterais à esquerda, módulo H, forma uma partição em G, com a pecularidade de que aqui as classes são conjuntos equipotentes. Se o conjunto das classes laterais à esquerda é finito, o número de classes à esquerda é igual ao de classes à direita Isto poderia ser provado mostrando que $aH \longmapsto Ha^{-1}$ é uma bijeção o que, aliás, vale em qualquer caso. No caso finito chamaremos de *índice* de H em G o número de classes laterais módulo H em G. Notação: (G : H).

Exemplo: Tomemos o grupo aditivo $\mathbb{Z}_6$ e consideremos o subgrupo $H = \{\bar{0}, \bar{2}, \bar{4}\}$. As classes módulo H, à esquerda ou à direita, pois G é comutativo, são

$$H = \bar{0} + H = \{\bar{0}, \bar{2}, \bar{4}\} \quad \text{e} \quad \bar{1} + H = \{\bar{1}, \bar{3}, \bar{5}\}$$

já que as outras que poderiam ser construídas coincidem com uma dessas. Então a partição de $\mathbb{Z}_6$ neste caso é feita por duas classes, cada uma com 3 elementos. Logo $(\mathbb{Z}_6 : H) = 2$.

3. TEOREMA DE LAGRANGE E COROLÁRIOS

Continuaremos a usar neste item a notação multiplicativa. Mas os grupos aqui considerados serão finitos.

Teorema 2 (Lagrange): Seja H um subgrupo de um grupo finito G. Então $o(H) \mid o(G)$ e $o(G) = o(H)(G : H)$.

Demonstração: Suponhamos $(G:H) = r$ e seja $\{a_1H, \ldots, a_rH\}$ o conjunto de todas as classes laterais à esquerda, módulo H. Então

$$a_1H \cup \ldots \cup a_rH = G$$

Como cada elemento de G figura numa e numa só dessas classes e como o número de elementos de cada classe é o(H) (proposição 19), então

$$r \cdot o(H) = o(G).$$

Como $r = (G:H)$ o teorema está provado. ■

Corolário 1: Sejam $a \in G$ e $H = [a]$. Então o período de a divide a ordem de G e o quociente nessa divisão é (G : H).

Demonstração: Basta lembrar que $o(a) = o(H)$ e que, devido ao teorema, $o(G) = o(H)(G:H)$. ■

Corolário 2: Se a é um elemento de G, então $a^{o(G)} = e$.

Demonstração: Seja $H = [a]$. Então $o(G) = o(H)(G : H) = o(a)(G : H)$. Mas $a^{o(a)} = e$. Donde

$$a^{o(G)} = (a^{o(a)})^{(G:H)} = e^{(G:H)} = e. \quad \blacksquare$$

Colorário 3: Todo grupo finito G, cuja ordem é um número primo p, é cíclico e seus únicos subgrupos são os triviais: G e $\{e\}$.

Demonstração: Como $p > 1$, então existe $a \in G$ tal que $a \neq e$. Logo $H = [a]$ é um subgrupo de G de ordem no mínimo igual a 2 : H contém *e* e *a* pelo menos. Como $o(H) \mid o(G)$ e $o(G)$ é um número primo, concluímos que $o(H) = p$. Disto segue que $H = G$ e, portanto, G é cíclico.

Por outro lado, como os subgrupos de G devem ter ordem 1 ou p (devido ao teorema), podemos afirmar que G só comporta mesmo os subgrupos triviais. ■

EXERCÍCIOS

84. Determinar todas as classes laterais de $H = \{\bar{0}, \bar{2}\}$ no grupo aditivo $\mathbb{Z}_4$.

85. Determinar todas as classes laterais de $3\mathbb{Z}$ no grupo aditivo $\mathbb{Z}$.

86. Seja S_3 o grupo das permutações de $E = \{1, 2, 3\}$. Determinar todas as classes laterais de $H = \{f_0, f_1\}$ subgrupo de S_3 onde

$$f_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \text{e} \quad f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

87. A) Seja G um grupo aditivo e H um subgrupo de G. Se $a, b \in G$, em que condições $a + H = b + H$?

B) Sendo $H = \{0, \pm m, \pm 2m, \ldots\}$, $m \in \mathbb{Z}$, um subgrupo do grupo aditivo $\mathbb{Z}$ mostre que $\{\bar{0}, \bar{1}, \ldots, \overline{m-1}\} = \mathbb{Z}_m$ é o conjunto das classes laterais de H. (Logo $(\mathbb{Z} : H) = m$.)

88. É finito ou infinito o número de classes de $\mathbb{Z} \times 2\mathbb{Z}$ em $\mathbb{Z} \times \mathbb{Z}$? Por que?

89. Dado o grupo $\mathbb{Z} \times \mathbb{Z}_2$ (produto direto), ache todas as classes laterais, à esquerda, do subgrupo $H = \{0\} \times \mathbb{Z}_2$.

90. Se H é um subgrupo de G tal que $(G : H) = 2$, mostre que $aH = Ha$, $\forall\, a \in G$.

Solução

Se $(G : H) = 2$ então existem em G duas classes laterais distintas que são H e $G - H$.

Dado $a \in G$, existem duas possibilidades:

1ª) $a \in H \Longrightarrow aH = H = Ha$

2ª) $a \in G - H \Longrightarrow aH = G - H = Ha$

91. Mostre que são equipotentes os conjuntos das classes laterais à esquerda e o das classes laterais à direita para todo subgrupo de um grupo G.

Sugestão: considerar $\varphi(aH) = Ha^{-1}$.

92. Aplique o corolário 2 e prove que no grupo multiplicativo $\mathbb{Z}_p^*$ (p primo) $\bar{a}^{(p-1)} = \bar{1}$ para todo $a \in \mathbb{Z} - \{p \cdot k \mid k \in \mathbb{Z}\}$. Daí conclua que se $p \nmid a$, então $a^{p-1} \equiv 1 \pmod{p}$.

93. Seja G um grupo de ordem p^n, onde p é primo e $n > 1$. Mostre que a ordem de um elemento qualquer de G é uma potência de p.

94. Sejam H e K subgrupos de um grupo finito. Se $o(H) = p$ e $o(K) = q$ ($p \neq q$ primos), então $H \cap K = \{e\}$. Prove.

95. Mostre que o número de classes laterais de $\mathbb{R}$ em $\mathbb{C}$ é infinito.

96. A) Mostre que

$$H = \left\{ \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} \mid c \in \mathbb{R}^* \right\} \text{ é um subgrupo do grupo } GL_2(\mathbb{R}).$$

B) Mostre que existem infinitas classes de H em G.

97. Considerando $\mathbb{Z}$ como subgrupo do grupo aditivo $\mathbb{Q}$, descrever as classes $\mathbb{Z} + (-1)$ e $\mathbb{Z} + \frac{1}{2}$.

98. Mostre que $a + \mathbb{Z}$ é uma classe lateral de $\mathbb{Z}$ em $\mathbb{R}$ ($a \in \mathbb{R}$), então existe $b \in \mathbb{R}$ tal que $0 \leqslant b < 1$ e $b + \mathbb{Z} = a + \mathbb{Z}$.

99. Mostre que dada $a \mathbb{R}_+^*$ ($a \in \mathbb{C}^*$), então existe $b \in \mathbb{C}^*$ tal que $|b| = 1$ e $b\,\mathbb{R}_+^* = a\,\mathbb{R}_+^*$.

100. Seja H um subgrupo de um grupo $(G, \cdot)$.

a) Mostre que "$x \sim y \iff x^{-1}y \in H$" define uma relação de equivalência em G.

b) Mostre que, $\forall\ a \in G$, $\bar{a} = aH$.

101. Seja $f: G \longrightarrow J$ um homomorfismo de grupos. Sendo S um subgrupo de J prove que $f^{-1}(S)$ é subgrupo de G tal que $N(f) \subset f^{-1}(S)$.

§ 5º — SUBGRUPOS NORMAIS — GRUPOS-QUOCIENTES

Os grupos que intervirão neste parágrafo são todos multiplicativos. Mas é evidente que, mudada a notação, os resultados que obteremos são válidos em geral: por exemplo, para grupos aditivos.

1. PRODUTO DE SUBCONJUNTOS DE UM GRUPO MULTIPLICATIVO

Definição 16: Seja G um grupo multiplicativo e consideremos dois subconjuntos A e B quaisquer de G. Indicaremos por AB e chamaremos de *produto* de A por B o seguinte subconjunto de G:

$$AB = \phi \text{ se } A = \phi \text{ ou } B = \phi$$

$$AB = \{xy \mid x \in A \text{ e } y \in B\}, \text{ se } A \neq \phi \text{ e } B \neq \phi.$$

É claro que $(A, B) \longmapsto AB$ é uma lei de composição interna no conjunto $\mathcal{P}(G)$ das partes de G. Para essa lei, chamada *multiplicação de subconjuntos* de G, valem as seguintes propriedades:

(a) associativa (por que ?)

(b) existe elemento neutro que é o subconjunto $\{e\}$, onde e é o elemento neutro de G.

Exemplo:

Seja $G = \{e, a, b, c\}$ um grupo de Klein. Sua tábua é a seguinte:

·	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Se $A = \{e, a\}$ e $B = \{b, c\}$, então $AB = \{eb, ec, ab, ac\} = \{b, c\}$.

Nota: É claro que se G é abeliano, então $AB = BA$, $\forall$ A, B $\subset$ G.

2. SUBGRUPOS NORMAIS

Definição 17: Um subgrupo N de um grupo G se diz *normal* de G se e somente se, $xN = Nx$, $\forall$ $x \in G$.

Notação: $N \lhd G$.

No caso de N ser subgrupo normal de G indicaremos por G/N o conjunto das classes laterais à esquerda (que é o mesmo das classes laterais à direita), módulo H, em G.

Exemplos:

1) Se G é comutativo todo subgrupo de G é normal.

2) Consideremos o grupo diedral $D_6 = \{e, a, a^2, b, ba, ba^2\}$ cuja tábua pode ser encontrada no exemplo (m), item 4, § 1, deste capítulo. O subgrupo $H = \{e, a, a^2\}$ (verifique que é subgrupo) é normal pois

$eH = \{e, a, a^2\} = He$ $\qquad$ $bH = \{b, ba, ba^2\} = Hb$

$aH = \{e, a, a^2\} = Ha$ $\qquad$ $(ba)H = \{b, ba, ba^2\} = H(ba)$

$a^2H = \{e, a, a^2\} = Ha^2$ $\qquad$ $(ba^2)H = \{b, ba, ba^2\} = H(ba^2)$

Sugerimos ao leitor verificar os cálculos na tábua.

Proposição 20: Seja N um subgrupo normal de G. Então G/N é fechado em relação à lei "multiplicação de subconjuntos de G". Mais precisamente vale a igualdade $(aN)(bN) = (ab)N$, $\forall$ a, b $\in$ G.

Demonstração: (i) $x \in (ab)N \Longrightarrow \exists\ n \in N \mid x = (ab)n \Longrightarrow x = (ae)(bn)$, onde $e, n \in N \Longrightarrow x \in (aN)(bN)$. Com isso ficou provado que $(ab)N \subset (aN)(bN)$.
(ii) $x \in (aN)(bN) \Longrightarrow \exists\ n_1, n_2 \in N \mid x = (an_1)(bn_2) = a(n_1 b)n_2$. Mas $n_1 b \in Nb = bN$. Donde $\exists\ n \in N \mid n_1 b = bn$. Portanto

$$x = a(bn)n_2 = (ab)(nn_2) \in (ab)N.$$

Isso nos garante a inclusão $(aN)(bN) \subset (ab)N$ o que vem concluir a demonstração. ■

3. GRUPOS QUOCIENTES

Seja N um subgrupo normal de G. Observemos que

a) $(aN)(bN) = (ab)N$, $\forall$ a, b $\in$ G;

b) $[(aN)(bN)](cN) = (aN)[(bN)(cN)]$, $\forall$ a, b, c $\in$ G (ver item 1);

c) $\forall\ a \in G \Longrightarrow (aN)(eN) = (eN)(aN) = aN$

d) $\forall\ a \in G \Longrightarrow (aN)(a^{-1}N) = (a^{-1}N)(aN) = eN = N$.

Isto tudo nos mostra que $(G/N, \cdot)$ é um grupo.

Definição 18: O grupo G/N obtido por meio das considerações anteriores é chamado *grupo quociente* de G por N. É claro que a existência de G/N pressupõe que N seja normal.

Exemplos:

1º) Se $G = \{1, i, -1, -i\}$ e $H = \{1, -1\}$, então $G/H = \{H, iH\}$ e a tábua deste grupo é a que está ao lado.

·	H	iH
H	H	iH
iH	iH	H

2º) Se $G = \mathbb{Z}_4$ e $H = \{\overline{0}, \overline{3}\}$ então, $G/H = \{H, \overline{1}+H, \overline{2}+H\}$ e a tábua deste grupo é a que está ao lado.

+	H	$\overline{1}+H$	$\overline{2}+H$
H	H	$\overline{1}+H$	$\overline{2}+H$
$\overline{1}+H$	$\overline{1}+H$	$\overline{2}+H$	H
$\overline{2}+H$	$\overline{2}+H$	H	$\overline{1}+H$

3º) Voltando ao exemplo 2 do item anterior onde $G = D_6$ e $H = \{e, a, a^2\}$, vemos que $G/H = \{H, bH\}$. A tábua deste grupo é

·	H	bH
H	H	bH
bH	bH	H

4. TEOREMA DO HOMOMORFISMO

Lema: Se f é um homomorfismo do grupo G no grupo J, então N(f) é um subgrupo normal de G.

Demonstração: Que é subgrupo já vimos anteriormente. Temos de provar que $xN = Nx$, $\forall\ x \in G$, onde $N = N(f)$.

$$y \in xN \Longrightarrow \exists\ n \in N \mid y = xn \Longrightarrow \exists\ n \in N \mid y = (xnx^{-1})x.$$

Mas

$$f(xnx^{-1}) = f(x)f(n)f(x^{-1}) = f(x)u(f(x))^{-1} = u \ (= \text{el. neutro de J})$$

o que significa que $xnx^{-1} \in N$. Portanto

$$y = (xnx^{-1})x \in Nx.$$

Mostramos assim que $xN \subset Nx$. É óbvio que também $Nx \subset xN$. ■

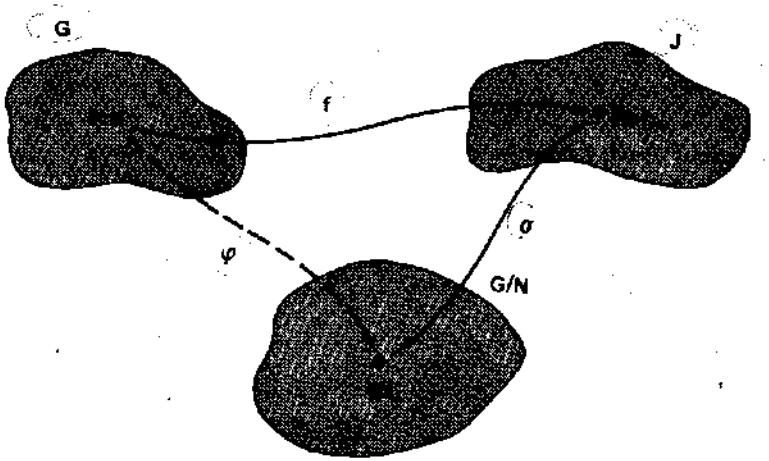
Teorema 3 (do homomorfismo): Seja f um homomorfismo sobrejetor (epimorfismo) do grupo G no grupo J. Se $N = N(f)$, então $G/N \simeq J$.

Demonstração: Consideremos a relação $aN \longrightarrow f(a)$ de G/N em J. Trata-se de uma aplicação injetora porque

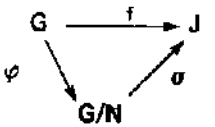
$aN = bN \iff a^{-1}b \in N \iff f(a^{-1}b) = u$ (el. neutro de J) $\iff (f(a))^{-1}f(b) = u \iff f(a) = f(b)$. Vamos dar o nome de σ a essa aplicação.

Dado $y \in J$, existe $x \in G$ de modo que $f(x) = y$. Tomando a classe xN, teremos $\sigma(xN) = f(x) = y$. Então σ é também sobrejetora.

Por último: $\sigma[(aN)(bN)] = \sigma[(ab)N] = f(ab) = f(a)f(b) = \sigma(aN)\,\sigma(bN)$. ■



Nota: A aplicação $\varphi : G \longrightarrow G/N$ dada por $\varphi(a) = aN$ é um homomorfismo de grupos pois $\varphi(ab) = (ab)N = (aN)(bN) = \varphi(a)\,\varphi(b)$, $\forall\ a, b \in G$. Este homomorfismo é chamado *homomorfismo canônico* de G sobre G/N e com ele podemos construir o seguinte diagrama de grupos e homomorfismos:



onde $f = \sigma \circ \varphi$, pois

$$(\sigma \circ \varphi)(a) = \sigma(aN) = f(a), \quad \forall\ a \in G.$$

EXERCÍCIOS

102. Seja G um grupo multiplicativo. Se $A \subset G$ $(A \neq \phi)$ seja $A^{-1} = \{ x^{-1} \mid x \in A \}$.
Mostre que:
a) $(A^{-1})^{-1} = A$ e
b) $\forall$ $A, B \subset G \mid A \neq \phi, B \neq \phi \implies (AB)^{-1} = B^{-1} \cdot A^{-1}$.

103. Seja G um grupo multiplicativo e $H \neq \phi$ um subconjunto de G. Mostre que:
H é subgrupo de G $\iff$ $H \cdot H \subset H$ e $H^{-1} \subset H$.

104. Seja $G = [a]$ um grupo cíclico de ordem 6. Sendo $H = [a^2]$, construa a tábua do grupo G/H.

Solução

$H = [a^2] = \{e, a^2, a^4\}$.
As classes laterais à esquerda, de H são:
$eH = H$ e $aH = \{a, a^3, a^5\}$.
Notemos que $eH = a^2H = a^4H$ e $aH = a^3H = a^5H$.
Observemos também que $xH = Hx$, $\forall \in G$, pois G é abeliano.
Podemos, então, construir a tábua de G/H:

·	H	aH
H	H	aH
aH	aH	H

105. Determinar todos os subgrupos não triviais do grupo aditivo $\mathbb{Z}_6$. Em cada caso construir o grupo quociente.

106. Construa a tábua dos seguintes grupos-quocientes:
a) $\mathbb{Z}_8/H$ onde $H = \{\overline{0}, \overline{4}\}$
b) $\mathbb{Z}/2\mathbb{Z}$

107. Seja G o grupo aditivo $\mathbb{Z} \times \mathbb{Z}$ (produto direto). Construa a tábua dos seguintes grupos-quocientes:
$G/(3\mathbb{Z} \times 2\mathbb{Z})$, e $G/(\mathbb{Z} \times \mathbb{Z})$, onde $2\mathbb{Z} = \{0, \pm 2, \pm 4, \ldots\}$ e $3\mathbb{Z} = \{0, \pm 3, \pm 6, \ldots\}$.

108. Se $N \lhd G$, $a \in G$ e $n \in N$, então existe um elemento $n' \in N$ tal que $an = n'a$.

109. Sejam M e N subgrupos normais de G. Mostre que $M \cap N$ e MN também o são.

Solução

Façamos $M \cap N = H$ e $MN = K$.
Sugerimos ao leitor mostrar que H e K são subgrupos de G.
Provemos que $xH = Hx$, $\forall \in G$;

$$\left.\begin{array}{l} y \in xH \implies y = xh \\ h \in M \cap N \end{array}\right\} \implies y = m'x = n'x$$

e, então, $m' = n' = h'$, isto é, $y = h'x \in Hx$
Analogamente, $y \in Hx \implies y \in xH$

Provemos que $xK = Kx$, $\forall \in G$:
$y \in xK \implies y = xk = x(mn) = (xm)n = (m'x)n = m'(xn) = m'(n'x) = (m'n')x = k'x \implies$
$\implies y \in Kx$
e, analogamente, $y \in Kx \implies y \in xK$

110. Mostre que um subgrupo N de G é normal, se, e somente se, $x^{-1}Nx = N$, $\forall$ $x \in G$.

111. Sejam M e N subgrupos normais de G tais que $M \cap N = \{e\}$. Mostre que $mn = nm$, $\forall$ $m \in M$ e $\forall$ $n \in N$.

Sugestão: Prove que $(mn)(nm)^{-1} = e$

112. Seja N um subgrupo de G tal que $(G:N) = 2$. Mostre que N é normal em G.

113. Seja G um grupo multiplicativo.
Mostre que $H = \{x \in G \mid xa = ax, \forall a \in G\}$ é um subgrupo normal de G.

Solução

1º) Sendo e o elemento neutro de G, temos $ea = ae$, $\forall$ $a \in G$, portanto, $e \in H$ e $H \neq \phi$.

2º) Sejam $x, y \in H$. Então, x e y comutam com qualquer elemento de G. Interessa particularmente observar que, se $a \in G$, então: $xa = ax$ e $ya^{-1} = a^{-1}y$.
Provemos que $xy^{-1} \in H$:
$(xy^{-1})a = x(y^{-1}a) = x(a^{-1}y)^{-1} = x(ya^{-1})^{-1} = x(ay^{-1}) = (xa)y^{-1} = (ax)y^{-1} = a(xy^{-1})$.

3º) Provemos finalmente que $aH = Ha$, $\forall$ $a \in G$:
$\alpha \in aH \iff \alpha = ah \iff \alpha = ha \iff \alpha \in Ha$
então $aH \subsetneq Ha$

114. Sejam G um grupo, H um subgrupo de G e N um subgrupo normal de G. Mostre que NH é um subgrupo de G e NH = HN.

115. Seja $f: G \longrightarrow J$ um homomorfismo sobrejetor de grupos. Se H é um subgrupo normal de G, mostre que f(H) é um subgrupo normal de J.

116. a) Mostre que, se Aut(G) indica o conjunto dos automorfismos de G, então (Aut(G), o) é um grupo.

b) Para cada $a \in G$ seja $F_a: G \longrightarrow G$ dada por $F_a(x) = axa^{-1}$, $\forall\ x \in G$. Mostre que $I(G) = \{F_a \mid a \in G\}$ é um subgrupo normal de Aut(G).

(*Nota:* cada elemento I(G) é chamado *Automorfismo interno* de G).

117. Seja T um subgrupo cíclico e normal de G. Mostre que todo subgrupo de T é subgrupo normal de G.

Capítulo III

ANÉIS E CORPOS

§ 1º — ANÉIS

1. CONCEITO DE ANEL

Sejam $(x, y) \longmapsto x + y$ e $(x, y) \longmapsto xy$ leis de composição internas num conjunto $A \neq \phi$. Suponhamos que

I) O conjunto A é um grupo abeliano em relação à primeira dessas leis (adição), isto é:

(a) $(\forall\ a, b, c \in A)(a + (b + c) = (a + b) + c)$

(b) $(\forall\ a, b \in A)(a + b = b + a)$

(c) Existe elemento neutro para essa adição. Será ele indicado por O_A ou apenas O, quando não houver possibilidade de confusão: é o *zero* do anel. Portanto, para todo $a \in A$, temos: $a + 0 = a$;

(d) Todo elemento de A admite um simétrico aditivo. Ou seja, para todo $a \in A$ existe um elemento em A, indicado por $(-a)$, de forma que $a + (-a) = 0$;

II) A segunda das leis consideradas (multiplicação) é associativa:

$$(\forall\ a, b, c \in A)(a(bc) = (ab)c);$$

III) A multiplicação é distributiva em relação à adição: $(\forall\ a, b, c \in A)$ $(a(b + c) = ab + ac$ e $(a + b)c = ac + bc)$.

Definição 1: Nas condições expostas dizemos que o conjunto A é um *anel* em relação à adição e à multiplicação consideradas. Ou ainda, que a terna ordenada formada pelo conjunto A, a adição e a multiplicação (resumidamente $(A, +, \cdot)$) é um *anel*. Às vezes diremos apenas "A é um anel" ou falaremos do

"anel A", por simplificação de linguagem, mas isso pressupõe, naturalmente, um par de leis de composição internas em A (com as propriedades citadas) sobre as quais não há nenhuma dúvida.

2. EXEMPLOS IMPORTANTES DE ANEL

(a) São exemplos clássicos de anel:

- $(\mathbb{Z}, +, \cdot)$, onde a adição e a multiplicação consideradas são as usuais. É o *anel dos inteiros*.
- *Anel dos racionais:* $(\mathbb{Q}, +, \cdot)$
- *Anel dos reais:* $(\mathbb{R}, +, \cdot)$
- *Anel dos complexos:* $(\mathbb{C}, +, \cdot)$

(b) Os conjuntos $n\mathbb{Z} = \{nq \mid q \in \mathbb{Z}\}$ $(n \in \mathbb{N};\ n \geqslant 1)$ são fechados em relação às operações usuais de $\mathbb{Z}$ pois

$$nq_1 + nq_2 = n(q_1 + q_2) \quad \text{e} \quad (nq_1)(nq_2) = n(nq_1q_2).$$

É fácil provar (fica como exercício) que, para cada $n \geqslant 1$, os seis axiomas da definição dada se verificam. Logo temos aí uma seqüência de anéis: $\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, \ldots$

(c) Cada conjunto $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$, $\forall\ m \in \mathbb{Z}, m > 1$, é um anel em relação às operações já definidas no capítulo 1

$$\overline{a} + \overline{b} = \overline{a + b}$$

$$\overline{a}\,\overline{b} = \overline{ab}, \quad \forall\ \overline{a}, \overline{b} \in \mathbb{Z}_m$$

As propriedades dessas duas leis, estudadas no capítulo citado, nos garantem que, de fato, $(\mathbb{Z}_m, +, \cdot)$ é um anel. O zero desse anel é $\overline{0}$ e o oposto de um elemento $\overline{a}$ é $\overline{m-a}$.

Nota: A título de simplificação escreveremos apenas $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ em várias oportunidades. Quando assim procedermos, para operar com os elementos de $\mathbb{Z}_m$ deveremos observar que

$a + b$ = resto na divisão euclidiana de $a + b$ $(\in \mathbb{Z})$ por m

e

ab = resto na divisão euclidiana de ab $(\in \mathbb{Z})$ por m.

Por exemplo, ao trabalhar em $\mathbb{Z}_4$ poderemos indicar os quatro elementos deste conjunto apenas por 0, 1, 2 e 3, ou seja, $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. Nessas condições teremos, por exemplo, $2 + 2 = 0$ e $2 \cdot 3 = 2$.

(d) *Anéis de Matrizes*

Consideremos os conjuntos $M_n(\mathbb{Z})(\forall n \geqslant 1)$. No capítulo I, § 1, quando dávamos exemplos de grupos, falamos dos grupos aditivos de matrizes e dos grupos lineares. Lá lembramos uma série de propriedades sobre matrizes quadradas: o suficiente para podermos dizer agora que cada $M_n(\mathbb{Z})$ é um anel em relação à adição e à multiplicação de matrizes nxn. Verifique.

Analogamente são anéis: $M_n(\mathbb{Q})$, $M_n(\mathbb{R})$ e $M_n(\mathbb{C})$.

De um modo geral, se A é um anel, podemos construir o conjunto $M_n(A)$ das matrizes nxn sobre A e transformar este conjunto num anel: é só generalizar o que se faz, por exemplo, com $M_n(\mathbb{Z})$.

Por exemplo, podemos construir o conjunto $M_2(\mathbb{Z}_3)$ das matrizes 2x2 sobre $\mathbb{Z}_3$. Trata-se de um anel com 3^4 elementos. Daremos a seguir algumas matrizes de $M_2(\mathbb{Z}_3)$:

$$A = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad C = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad D = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$$

Observe que, por exemplo,

$$A + D = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{e} \quad AD = \begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix}$$

(e) *Anéis de Funções*

Seja $A = \mathbb{Z}^{\mathbb{Z}} = \{f \mid f : \mathbb{Z} \longrightarrow \mathbb{Z}\}$. Dadas duas funções quaisquer $f, g \in A$, definindo $f + g$ e fg da seguinte maneira

$$f + g : \mathbb{Z} \longrightarrow \mathbb{Z} \quad \text{e} \quad (f + g)(x) = f(x) + g(x), \quad \forall\ x \in \mathbb{Z}$$

$$fg : \mathbb{Z} \longrightarrow \mathbb{Z} \quad \text{e} \quad (fg)(x) = f(x)\,g(x), \quad \forall\ x \in \mathbb{Z}$$

temos definidas uma "adição" e uma "multiplicação" em A. Nessas condições A é um anel: o anel das funções de $\mathbb{Z}$ em $\mathbb{Z}$. Verifiquemos alguma coisa dessa afirmação.

O zero desse anel é a função $x \longmapsto 0$, que indicaremos apenas por 0 uma vez que $(f + 0)(x) = f(x) + 0(x) = f(x) + 0 = f(x)$, $\forall\ x \in \mathbb{Z}$. O simétrico aditivo de uma função $f \in A$ é a função dada por $x \longmapsto -f(x)$ a qual se indica por $(-f)$. De fato:

$$(f + (-f))(x) = f(x) + (-f)(x) = f(x) - f(x) = 0 = 0(x).$$

A propriedade associativa da adição se verifica da seguinte maneira:

$\forall\ f, g, h \in A$ e $\forall\ x \in \mathbb{Z}$,

$((f + g) + h)(x) = (f + g)(x) + h(x) = (f(x) + g(x)) + h(x) \overset{*}{=} f(x) + (g(x) + h(x)) =$

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

* Propriedade associativa da adição em $\mathbb{Z}$.

Analogamente se constroem os anéis $\mathbb{Q}^{\mathbb{Q}}$, $\mathbb{R}^{\mathbb{R}}$ e $\mathbb{C}^{\mathbb{C}}$. De uma maneira mais geral, se X é um conjunto não vazio e se A é um anel, então $A^X = \{f \mid f:X \longrightarrow A\}$ é um anel.

(f) *Produtos Diretos*

Sejam A e B anéis quaisquer. Se definirmos "soma" e "produto" de elementos de AxB do seguinte modo

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

e

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2)$$

$\forall\ (a_1, b_1), (a_2, b_2) \in AxB$, é fácil provar (fica como exercício) que $(AxB, +, \cdot)$ é um anel cujo zero é $(0_A, 0_B)$ e cujo oposto de um elemento (a, b) é (-a, -b), onde -a é o oposto de a em A e -b é o oposto de b em B.

O anel assim obtido chama-se *produto direto* externo de A e B.

Nota: Dados os anéis A e B, quando nos referirmos ao anel AxB, sem nenhuma outra menção, trata-se do produto direto de A por B aqui definido.

3. PRIMEIRAS PROPRIEDADES DE UM ANEL

Consideremos um anel $(A, +, \cdot)$

(a) Quanto à adição, A é um grupo abeliano; então são verdadeiras as seguintes propriedades já vistas para grupos (cap. II - § 1 - 5):

- o zero do anel A é único
- para cada $a \in A$ existe um único simétrico aditivo
- dados $a_1, \ldots, a_n \in A$ $(n \geqslant 2)$, $-(a_1 + \ldots + a_n) = (-a_1) + \ldots + (-a_n)$ (observar que aí já usamos a comutatividade da adição)
- $(\forall\ a \in A)\ (-(-a) = a)$
- $(\forall\ a, x, y \in A)(a + x = a + y \implies x = y)$ (Vale a lei do cancelamento da adição)
- o conjunto-solução de uma equação $a + x = b$, onde a e b são elementos dados de A e x é variável em A é $\{(-a) + b\}$

(b) $(\forall\ a)(a \in A \implies a0 = 0a = 0)$

Justificação: $0 + a0 = a0 = a(0 + 0) = a0 + a0$

$0 = a0$ (em virtude da lei do cancelamento da adição).

Analogamente se prova que $0a = 0$. ■

(c) $(\forall\ a, b)(a, b \in A \implies a(-b) = (-a)b = -(ab))$

Justificação: $ab + [-(ab)] = 0 = a0 = a[b + (-b)] = ab + a(-b)$

$-(ab) = a(-b)$

(mesmo motivo da prop. anterior)

Analogamente se prova que $-(ab) = (-a)b$ (exercício). ■

(d) $(\forall\ a, b)(a, b \in A \implies ab = (-a)(-b))$

Justificação: $(-a)(-b) = -[(-a)b] = -[-(ab)] = ab$. Notar que nas duas primeiras passagens usamos o resultado anterior. ■

Definição 2 (*diferença* entre dois elementos): Dados dois elementos a e b de um anel A, a *diferença* entre a e b, que indicaremos por $a - b$, é o elemento $a + (-b)$. Assim $a - b = a + (-b)$.

(e) $(\forall\ a, b, c)(a, b, c \in A \implies a(b - c) = ab - ac)$

Justificação: $a(b - c) = a[b + (-c)] = ab + a(-c) = ab + [-(ac)] = ab - ac$. ■

Definição 3 (*potenciação* num anel): Dados $a \in A$ e $n \in \mathbb{N}^*$, define-se a^n por recorrência do seguinte modo:

$$a^1 = a \quad \text{e} \quad a^n = a^{n-1}a \quad (\forall\ n > 1).$$

(f) $(\forall\ a \in A \text{ e } \forall\ m, n \in \mathbb{N}^*)(a^m a^n = a^{m+n})$

Justificação: (indução sobre n): Suponhamos $n = 1$. Então, $a^m a^1 = a^m a = a^{m+1}$, pela própria definição. Suponhamos $a^m a^r = a^{m+r}$. Então

$$a^m a^{r+1} = a^m(a^r a^1) = (a^m a^r)a^1 = a^{m+r}a = a^{(m+r)+1} = a^{m+(r+1)}$$ ■

(g) $(\forall\ a \in A \text{ e } \forall\ m, n \in \mathbb{N}^*)((a^m)^n = a^{mn})$

Justificação: $(a^m)^1 = a^m$, por definição. Suponhamos $(a^m)^r = a^{mr}$, com $r \geqslant 1$. Então

$$(a^m)^{r+1} = (a^m)^r a^m = a^{mr}a^m = a^{mr+m} = a^{m(r+1)}$$ ■

4. SUBANÉIS

Definição 4: Seja $(A, +, .)$ um anel. Dizemos que um subconjunto $L \subset A$, $L \neq \phi$, é um *subanel* de A se, e somente se,

(i) L é fechado para ambas as operações de A, isto é,

$$(\forall\ a, b)(a, b \in A \implies a + b \in L \ \text{ e } \ ab \in L)$$

(ii) $(L, +, .)$ também é um anel. (A adição e a multiplicação aí indicadas são as mesmas do anel A, só que restritas a L, como é evidente).

Exemplos:

1) $2\mathbb{Z}$ é um subanel de $\mathbb{Z}$.

De fato, a soma e o produto de dois números pares são números pares. Além disso, tanto a adição como a multiplicação de números pares são associativas, a adição é comutativa, o número zero é par e o oposto de um número par é também um número par. Finalmente a multiplicação de números pares é distributiva em relação à adição (explique).

2) $M_n(\mathbb{Z})$ é um subanel de $M_n(\mathbb{R})$. Por que?

Proposição 1: Sejam A um anel e L um subconjunto de A. Então L é um subanel de A se, e somente se,

$$(\forall\ a, b)(a, b \in L \implies a - b \in L \ \text{ e } \ ab \in L)$$

ou seja, L é fechado para a subtração e para a multiplicação de A.

Demonstração: ($\implies$) Por hipótese $(L, +)$ é um subgrupo do grupo $(A, +)$. Logo

$$(\forall\ a, b)(a, b \in L \implies a - b \in L)$$

Por hipótese, ainda, L é fechado para a multiplicação de A. Isto conclui a demonstração quanto a esta parte.

($\impliedby$) Da hipótese

$$a, b \in L \implies a - b \in L$$

decorre que L é um subgrupo de $(A, +)$. Logo $(L, +)$ é um grupo abeliano.

Por outro lado, como $L \subset A$ e L é fechado para a multiplicação de A, então $(\forall\ a, b, c)(a, b, c \in L \implies a, b, c \in A \implies a(bc) = (ab)c)$ é a propriedade associativa da multiplicação em L e

$(\forall\ a, b, c)(a, b, c \in L \implies a, b, c \in A \implies a(b + c) = ab + ac \ \text{ e } \ (a + b)c = ac + bc)$ é a propriedade distributiva da multiplicação em relação à adição em L. ■

Exemplo: Verifiquemos que $L = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$ é subanel de $M_2(\mathbb{R})$.

É claro que $L \neq \phi$. Dadas $X = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ e $Y = \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix}$ em L, então:

$$X - Y = \begin{pmatrix} a - c & b - d \\ 0 & 0 \end{pmatrix} \in L \ \text{ e } \ X \cdot Y = \begin{pmatrix} ac & ad \\ 0 & 0 \end{pmatrix} \in L.$$

Verificando-se para L as hipóteses da proposição 1 podemos afirmar que L é subanel de L.

Dessa maneira chegamos à conclusão de que $(L, +, .)$ é um anel de uma maneira muito mais rápida do que pela definição com seus seis axiomas.

5. ANÉIS COMUTATIVOS — ANÉIS COM UNIDADE

Definição 5: Dizemos que um anel A é um *anel comutativo* se a sua multiplicação é comutativa, isto é

$$(\forall\ a, b)(a, b \in A \implies ab = ba)$$

Exemplos: São anéis comutativos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $n\mathbb{Z}$, $\mathbb{Z}_m$ e A^X (toda vez que A é comutativo). Se A e B são comutativos, então AxB (produto direto de A por B) também é comutativo. O anel $M_2(\mathbb{Z})$, por exemplo, não é comutativo. Tomando

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \ \text{ e } \ B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

então

$$AB = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \ \text{ e } \ BA = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Definição 6: Um *anel com unidade* é um anel A que conta com elemento neutro para a multiplicação. Este elemento será indicado por 1_A ou apenas por 1, se não houver possibilidade de confusão. Suporemos sempre que $1_A \neq 0_A$. Um *anel comutativo com unidade* é um anel cuja multiplicação é comutativa e para a qual exista elemento neutro. O elemento neutro da multiplicação de um anel é chamado, quando existe, de *unidade* do anel.

Exemplos: os anéis $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ possuem unidade. Para todos eles é claro que é o número 1. O anel $M_n(\mathbb{Z})$ também possui unidade. É a matriz

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

Em geral, se A é um anel com unidade 1_A o anel M(A) também possui unidade que é a matriz

$$\begin{pmatrix} 1_A & 0_A & \dots & 0_A \\ 0_A & 1_A & \dots & 0_A \\ \dots & \dots & \dots & \dots \\ 0_A & 0_A & \dots & 1_A \end{pmatrix}$$

Observe-se ainda que $\overline{1}$ é a unidade de $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \dots, \overline{m-1}\}$ e que os anéis $n\mathbb{Z}$ não admitem unidade, salvo se $n = 1$, caso em que se trata do próprio $\mathbb{Z}$. Quando ao produto direto de dois anéis A e B, se estes forem dotados de unidade, o par $(1_A, 1_B)$ será a unidade de AxB.

Se o anel A possui unidade, então A^X também é um anel com unidade. De fato, observemos a aplicação $e: X \longrightarrow A$ dada por $e(x) = 1_A$, $\forall\ x \in A$. Se f é uma função qualquer de A^X, então

$$(fe)(x) = f(x)\,e(x) = f(x)1_A = f(x),\ \forall\ x \in X.$$

Logo a função e é a unidade neste caso.

Nota: Num anel com unidade define-se potência com expoente natural, por recorrência, da seguinte maneira:

$$a^0 = 1_A \qquad \text{e} \qquad a^n = a^{n-1}a,\ \forall\ n \geq 1.$$

A partir dessa definição demonstra-se, de maneira análoga ao que fizemos para provar as propriedades (f) e (g) do item 3, que

$$a^m a^n = a^{m+n} \qquad \text{e} \qquad (a^m)^n = a^{mn}$$

para todo $a \in A$ e para quaisquer $m, n \in \mathbb{N}$.

6. SUBANÉIS UNITÁRIOS

Sejam A um anel e L um subanel de A. Suponhamos que A é um anel com unidade. Quanto a L poderá então acontecer o seguinte: ou não tem unidade, ou tem unidade igual à de A ou L tem unidade e esta é diferente da de A. Vejamos alguns exemplos:

- $2\mathbb{Z}$ é um subanel de $\mathbb{Z}$. Existe a unidade de $\mathbb{Z}$ mas não existe a de $2\mathbb{Z}$.
- $\mathbb{Z}$ é subanel de $\mathbb{Q}$ e ambos admitem a mesma unidade.
- Considerando o produto direto $\mathbb{Z}x\mathbb{Z}$ é fácil verificar que $\{0\}x\mathbb{Z}$ é um subanel de $\mathbb{Z}x\mathbb{Z}$. Contudo, enquanto que (1, 1) é a unidade de $\mathbb{Z}x\mathbb{Z}$, a de $\{0\}x\mathbb{Z}$ é (0, 1) pois $(0, 1)(0, b) = (0, b)$, $\forall\ (0, b) \in \{0\}x\mathbb{Z}$.
- Seja B um subanel com unidade do anel $\mathbb{R}$. Como $1 \cdot 1_B = 1_B = 1_B \cdot 1_B$, então $1 = 1_B$.

Se A é um anel com unidade e se B é um subanel de A tal que existe unidade de B e $1_A = 1_B$, então diremos que B é um *subanel unitário* de A.

EXERCÍCIOS

1. Consideremos em $\mathbb{Z}x\mathbb{Z}$ as operações + e · , definidas por:
   $(a, b) + (c, d) = (a + c; b + d)$ e $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$
   Mostrar que $(\mathbb{Z}x\mathbb{Z}, +, \cdot)$ é um anel com unidade e comutativo.

2. Consideremos as operações $*$ e Δ em $\mathbb{Q}$, definidas por:
   $x * y = x + y - 3$ e $x \Delta y = x + y - \frac{xy}{3}$
   Mostrar que $(\mathbb{Q}, *, \Delta)$ é um anel comutativo com elemento unidade.

3. Prove que são anéis:
   A) o conjunto $\mathbb{Z}$ dotado das leis adição usual e a multiplicação assim definida
   $ab = 0;\ \forall\ a, b \in \mathbb{Z}$.
   B) o conjunto $\mathbb{Q}$ com as leis definidas por $x \oplus y = x + y - 1$ e $x \odot y = x + y - xy$.
   Observação: A "adição" e "multiplicação" consideradas aqui estão sendo indicadas por $\oplus$ e $\odot$ obviamente para evitar confusão com as usuais respectivas.
   C) o conjunto $\mathbb{Z}x\mathbb{Z}$ em relação à leis dadas assim:
   $(a, b) + (c, d) = (a + c, b + d)$ e $(a, b) \cdot (c, d) = (ac, ad + bc)$.

4. Quais dos anéis do exercício anterior são comutativos? Quais têm unidade? Determinar a unidade no caso de existir.

5. Consideremos as operações $*$ e Δ em $\mathbb{Z}$ definidas por:
$x * y = x + ay - 2$ e $x \Delta y = xy + bx + cy + d$, onde a, b, c, d são números inteiros dados. Determinar a, b, c, d de modo que $(\mathbb{Z}, *, \Delta)$ seja um anel. Para os valores obtidos de a, b, c, d, $(\mathbb{Z}, *, \Delta)$ é um anel comutativo com unidade?

6. Sabe-se que $A = \{a, b, c, d\}$ e $(A, +, \cdot)$ é um anel em que os elementos neutros das operações $+$ e $\cdot$ são, respectivamente, a e b. Conhecendo-se os compostos $b + b = a$, $c + c = a$, $dd = a$, construir as tábuas das duas operações.

7. Seja E um conjunto não vazio. Mostre que $A = \mathcal{P}(E)$ é um anel comutativo com unidade desde que se defina
$x + y = \complement_{(x \cup y)}(x \cap y)$ = complementar de $x \cap y$ em relação a $x \cup y$ e
$x \cdot y = x \cap y$, $\forall x, y \in A$.

8. Dê exemplo de um anel com 4 elementos todos satisfazendo a condição $x^2 = x$.

9. Verifique se existe um anel $A = \{a, b, c, d\}$ tal que $(A, +)$ é isomorfo como grupo ao $\mathbb{Z}_4$ e $x^2 = x$, $\forall x \in A$.

10. Seja A um anel cujas duas leis de composição são iguais, isto é, $a + b = ab$, $\forall a, b \in A$. Mostre que $A = \{0\}$.

11. Seja A um anel. Mostre que $\forall a, b, c \in A \implies a(b - c) = ab - ac$ e $(a - b)c = ac - bc$.

12. *Seja $(A, +, \cdot)$ um anel com unidade. Mostre que a comutatividade da adição é conseqüência dos demais axiomas que compõem a definição de anel.*
Sugestão: Prove que $(a + b) - (b + a) = 0$.

13. Sendo a e b elementos de um anel comutativo A mostre que
$(a + b)^n = a^n + \binom{n}{1} a^{n-1}b + \ldots + \binom{n}{1} ab^{n-1} + b^n$, $\forall n \geq 0$, $n \in \mathbb{Z}$.

14. Seja A um anel com a seguinte propriedade: $x^2 = x$, $\forall x \in A$. Mostre que: $-x = x$, $\forall x \in A$.
Sugestão: Considere o produto $(x + x)^2$.

15. *Prove que um anel A com a propriedade do exercício anterior é necessariamente comutativo.*
Sugestão: Tome $x, y \in A$ e calcule $(x + y)^2$.

16. Determinar quais dos seguintes subconjuntos de $\mathbb{Q}$ são subanéis:
a) $\mathbb{Z}$
b) $B = \{x \in \mathbb{Q} \mid x \notin \mathbb{Z}\}$
c) $C = \left\{\frac{a}{b} \in \mathbb{Q} \mid a \in \mathbb{Z}, b \in \mathbb{Z}, 2 \mid b\right\}$
d) $D = \left\{\frac{a}{2^n} \in \mathbb{Q} \mid a \in \mathbb{Z} \text{ e } n \in \mathbb{Z}\right\}$.

17. Verifique se são subanéis:
a) $L = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ do anel $\mathbb{R}$.
b) $\mathbb{Z}$ do anel do exercício 3B
c) $2\mathbb{Z} \times 2\mathbb{Z}$ do exercício 3C
d) Sendo $E = \mathbb{Z}$ e $A = \mathcal{P}(E)$ o subconjunto L das partes finitas de $\mathbb{Z}$.

18. Quais dos conjuntos abaixo são subanéis de $M_2(\mathbb{R})$?

$$L_1 = \left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in \mathbb{R}\right\}$$

$$L_2 = \left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R}\right\}$$

$$L_3 = \left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{R}\right\}$$

$$L_4 = \left\{\begin{pmatrix} 0 & a \\ c & b \end{pmatrix} \mid a, b, c \in \mathbb{R}\right\}$$

19. Dê exemplos de anéis A e subanéis B de forma que:
a) $\exists\ 1_A$ $\exists\ 1_B$ e $1_A = 1_B$
b) $\exists\ 1_A$ $\exists\ 1_B$ e $1_A \neq 1_B$
c) $\exists\ 1_A$ e $\nexists\ 1_B$
d) $\nexists\ 1_A$ e $\exists\ 1_B$
e) $\nexists\ 1_A$ e $\nexists\ 1_B$

20. Obter todos subanéis do anel $\mathbb{Z}_6$.
Sugestão: Determine todos os subgrupos de $(\mathbb{Z}_6, +)$ e verifique quais são fechados para a multiplicação.

21. Obter todos os subanéis do anel $\mathcal{P}(\{a, b, c\})$.

22. Se B e C são subanéis de A, então $B \cap C$ é subanel de A. Prove.

23. Se B é um subanel de A, então:
I) $a \in B$ e $n \in \mathbb{Z} \implies na \in B$.
II) $a \in B$ e $n \in \mathbb{N} \implies a^n \in B$.

§ 2º — ANÉIS DE INTEGRIDADE — CORPOS

1. ANÉIS DE INTEGRIDADE

Consideremos o anel $\mathbb{Z}$ dos inteiros e o anel $\mathbb{Z}^{\mathbb{Z}}$, por exemplo, das funções de $\mathbb{Z}$ em $\mathbb{Z}$. Ambos são anéis comutativos com unidade. Contudo há uma diferença fundamental entre os dois. Enquanto que no anel $\mathbb{Z}$ é verdadeira a frase

$$(\forall\ a, b \in \mathbb{Z})(ab = 0 \implies a = 0 \text{ ou } b = 0)$$

no anel $\mathbb{Z}^{\mathbb{Z}}$ não acontece o mesmo. De fato, consideremos as funções f e g de $\mathbb{Z}$ em $\mathbb{Z}$ dadas por

$$f(0) = 1 \text{ e } f(x) = 0,\ \forall\ x \neq 0, \text{ e}$$
$$g(0) = 0 \text{ e } g(x) = 1,\ \forall\ x \neq 0.$$

Trata-se obviamente de duas funções não nulas. Apesar disso o produto fg é nulo pois

$$(fg)(0) = f(0)g(0) = 1 \cdot 0 = 0$$

e, para todo $x \neq 0$,

$$(fg)(x) = f(x)g(x) = 0 \cdot 1 = 0$$

Esse tipo de observação motiva a definição a seguir.

Definição 7: Um anel A, comutativo com unidade, onde é verdadeira a seguinte frase

$$(\forall\ a, b \in A)(ab = 0_A \implies a = 0_A \text{ ou } b = 0_A)$$

recebe o nome de *anel de integridade*. A frase destacada na linha acima é chamada lei do *anulamento do produto*. Logo, um anel de integridade é um anel comutativo com unidade em que vale a lei do anulamento do produto. Se a e b são elementos não nulos de um anel A tais que $ab = 0_A$ ou $ba = 0_A$, dizemos que *a* e *b* são *divisôres próprios do zero* em A.

Exemplo: No anel $\mathbb{Z}_6$ os elementos $\overline{2}$ e $\overline{3}$ são divisores próprios do zero porque são não nulos e, no entanto, $\overline{2} \cdot \overline{3} = \overline{0}$.

Proposição 2: Um anel A, comutativo com unidade, é um anel de integridade se, e somente se, todo elemento não nulo de A é regular quanto à multiplicação, isto é,

$$(\forall\ a, b, c \in A)(a \neq 0 \text{ e } ab = ac \implies b = c) \quad (*)$$

Demonstração: ($\Longrightarrow$) Tomando $a \neq 0$ e supondo $ab = ac$, com $a, b, c \in A$, então $a(b - c) = 0$. Devido à hipótese podemos concluir então que $b - c = 0$. Donde $b = c$.

($\Longleftarrow$) Se existissem a, b $\in$ A, ambos não nulos, de maneira que $ab = 0$, teríamos $ab = a0$. Daí (hipótese): $b = 0$. Absurdo. ■

(*) Tais elementos são chamados elementos regulares do anel.

Exemplo importante: Já sabemos que todo anel $\mathbb{Z}_m$ de classes de restos é um anel comutativo com unidade. Mostraremos a seguir que $\mathbb{Z}_m$ é anel de integridade se, e somente se, m é primo.

($\Longrightarrow$) Se m não fosse primo, existiriam r, s $\in \mathbb{Z}$, de tal forma que $1 < r, s < m$ e $rs = m$. Daí $\overline{0} = \overline{m} = \overline{rs}$. Quer dizer, existiriam divisores próprios do zero em $\mathbb{Z}_m$ o que seria contrário à hipótese.

($\Longleftarrow$) Suponhamos que existissem $\overline{a}, \overline{b} \in \mathbb{Z}_m$ tais que $\overline{ab} = \overline{0}$. Então m | ab. Como m é primo, conclui-se que m | a ou m | b. Isto significa que $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$.

Outros exemplos

a) Os anéis $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são exemplos clássicos de anéis de integridade.

b) O anel $M_2(\mathbb{R})$ não é de integridade: além de não ser comutativo apresenta divisores próprios do zero, conforme se pode ver a seguir:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Note-se que

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

c) O produto direto $\mathbb{Z} \times \mathbb{Z}$ também não é anel de integridade, embora seja comutativo com unidade. Observe-se que

$$(a, 0) \cdot (0, b) = (0, 0)$$

mesmo quando $a, b \in \mathbb{Z}^*$.

2. CORPOS

Os anéis $\mathbb{Z}$ e $\mathbb{Q}$ são ambos comutativos com unidade. Para ambos vale a lei do anulamento do produto. Mas, enquanto que no anel $\mathbb{Z}$ somente o 1 e o -1 admitem simétrico multiplicativo, no anel $\mathbb{Q}$ todo elemento não nulo admite simétrico multiplicativo. Fatos como esse sugerem a definição a seguir.

Definição 8: Um anel K, comutativo com unidade, recebe o nome de *corpo* se todo elemento não nulo de K admite simétrico multiplicativo. Ou seja:

$$(\forall\ a \in K)(a \neq 0 \implies \exists\ b \in K \mid ab = 1).$$

O elemento b que apareceu na frase acima é chamado *inverso* de a e será indicado, daqui para a frente, por a^{-1}.

Num anel A com unidade indicaremos por U(A) o subconjunto de A formado pelos elementos para os quais existe simétrico multiplicativo (inverso). Esses elementos são chamados de *inversíveis*. Assim, um corpo K é um anel comutativo com unidade tal que $U(K) = K^* = K - \{0\}$.

Exemplos:

O anel $\mathbb{Z}$ não é um corpo. Como já vimos $U(\mathbb{Z}) = \{1, -1\}$.

Os anéis $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são corpos.

O anel $\mathbb{R}^{\mathbb{R}}$ das funções de $\mathbb{R}$ em $\mathbb{R}$ é comutativo, possui unidade, mas não é um corpo. De fato. Consideremos a função $f: \mathbb{R} \longrightarrow \mathbb{R}$ dada por $f(0) = 0$ e $f(x) = 5$, $\forall\ x \neq 0$. Essa função não é inversível uma vez que não existe nenhuma função $g: \mathbb{R} \longrightarrow \mathbb{R}$ de maneira que $fg = e$ (função constante 1), pois isto, se possível, implicaria

$$(fg)(0) = f(0)g(0) = 0 \cdot g(0) = 0 = e(0) = 1$$

o que é absurdo.

Proposição 3: Todo corpo K é um anel de integridade.

Demonstração: Sejam a e b elementos de K tais que $ab = 0$. Suponhamos que um deles, por exemplo a, é não nulo. Então existe $a^{-1} \in K$. Donde

$$a^{-1}(ab) = a^{-1}0$$

o que tem como consequência que $(a^{-1}a)b = 0$ e, então, $b = 0$.

Assim provamos que vale a lei do anulamento do produto em K. ■

Nota: A recíproca desse teorema não vale. Por exemplo, Z é anel de integridade mas não é corpo. Com uma certa restrição, contudo, ela passa a ser verdadeira. Vejamos.

Proposição 4: Todo anel de integridade finito é um corpo.

Demonstração: Seja $K = \{a_1, a_2, \ldots, a_n\}$ um anel de integridade formado de n elementos. Para todo $a \in K$, $a \neq 0$, a aplicação

$$a_i \longrightarrow aa_i$$

é injetora, de K nele próprio, uma vez que

$$aa_i = aa_j \Longrightarrow a_i = a_j.$$

Como K é finito essa aplicação é também sobrejetora, do que resulta

$$aK = \{aa_1, aa_2, \ldots, aa_n\} = K$$

Então a unidade de K poderá ser expressa do seguinte modo:

$1 = aa_r$, onde a_r é um elemento conveniente de K.

Dessa forma mostramos que para todo elemento não nulo $a \in K$ existe inverso. ■

3. QUOCIENTES NUM CORPO

Dados os elementos *a* e *b* de um corpo K, se $b \neq 0$ é comum indicar o elemento ab^{-1} por $\frac{a}{b}$. Estes *quocientes* (é como são chamados tais elementos) apresentam propriedades muito parecidas com as dos números racionais o que, de uma certa forma, explica a notação adotada.

Proposição 5: Sejam a, b, c e d elementos não nulos de um corpo K. Se $b \neq 0$ e $d \neq 0$, então

(a) $\frac{a}{b} = \frac{c}{d} \iff ad = bc$

(b) $\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}$

(c) $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$

(d) $\frac{a}{b} + \frac{-a}{b} = 0$

(e) Se $a \neq 0$ (além de b), então $\frac{a}{b}\frac{b}{a} = 1$

Demonstração

(a) ($\Longrightarrow$) Por hipótese $ab^{-1} = cd^{-1}$. Donde

$$ad = a(b^{-1}b)d = (ab^{-1})(bd) = (cd^{-1})(bd) = bc$$

($\Longleftarrow$) Por hipótese $ad = bc$. Daí

$$\frac{a}{b} = ab^{-1} = a(dd^{-1})b^{-1} = (ad)(d^{-1}b^{-1}) = (bc)(d^{-1}b^{-1}) = cd^{-1} = \frac{c}{d}.$$

(b) $$\frac{a}{b} \pm \frac{c}{d} = ab^{-1} \pm cd^{-1} = add^{-1}b^{-1} \pm cbb^{-1}d^{-1} = (ad \pm bc)(bd)^{-1} = \frac{ad \pm bc}{bd}$$

Deixamos como exercício a demonstração de (c), (d) e (e). ■

EXERCÍCIOS

24. Determinar o conjunto dos elementos regulares e o conjunto dos elementos inversíveis de cada um dos seguintes anéis:

a) $\mathbb{Z}$
b) $\mathbb{Q}$
c) $\mathbb{Z} \times \mathbb{Z}$ (produto direto)
d) $\mathbb{Z}_3$
e) $\mathbb{Z}_4$
f) $\mathbb{Z}_{14}$
g) $M_2(\mathbb{R})$
h) $\mathbb{Z}_2 \times \mathbb{Z}_3$

25. Seja R(A) o conjunto dos elementos regulares em relação à multiplicação do anel A. Provar que R(A) é fechado para a multiplicação e que R(A) = U(A) quando A é finito.

26. Ache os elementos inversíveis dos seguintes anéis:

a) $(\mathbb{Q}, \oplus, \odot)$, onde $a \oplus b = a + b - 1$ e $a \odot b = a + b - ab$

$(\mathbb{Q}, \oplus, \odot)$ é um corpo?

b) $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ onde $(a, b) + (c, d) = (a + c, b + d)$ e $(a, b) \cdot (c, d) = (ac, ad + bc)$.

27. Determine os divisores próprios de zero do anel $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ do exercício anterior.

28. Dê exemplo de um anel com unidade onde só a unidade é inversível.

29. a) Quais são os elementos inversíveis do anel $\mathbb{Z}_{18}$?

b) Resolver em $\mathbb{Z}_{18}$ o sistema:

$$\begin{cases} \overline{5}x + \overline{2}y = \overline{1} \\ x + \overline{11}y = \overline{7} \end{cases}$$

30. Um elemento a de um anel A se diz idempotente se $a^2 = a$ e nilpotente se existe $n \in \mathbb{N}$, de modo que $a^n = 0$. Mostre que o único elemento não nulo e idempotente de um anel de integridade é a unidade e que o zero é o único elemento nilpotente de um anel de integridade.

31. Obter o conjunto dos elementos nilpotentes dos seguintes anéis: $\mathbb{Z}$, $\mathbb{Z}_6$, $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$ e $\mathbb{R}^{\mathbb{R}}$.

32. Mostrar que o conjunto dos elementos nilpotentes de um anel comutativo A é um subanel de A.

33. Se E é um conjunto não vazio mostre que no anel $A = \mathcal{P}(E)$ todos os elementos são idempotentes.

34. Prove detalhadamente o seguinte: se $a \in A$ (anel de integridade) e $a^2 = 1$, então $a = 1$ ou $a = -1$.

35. Mostrar que se A é um anel de integridade, $x \in A$ e $x^2 = x$, então $x = 0$ ou $x = 1$.

36. Seja A um anel com unidade tal que $x^2 = x$, $\forall\ x \in A$. Mostre que A é um anel de integridade se, e somente se, $A = \{0, 1\}$.

37. Verdadeiro ou falso: se A é um anel de integridade e L é um subanel de A, então $1_A = 1_L$? Justifique.

38. Seja A um anel que possui um elemento e tal que $e^2 = e$, e não é um divisor próprio de zero de A. Mostre que e é unidade de A.

39. Seja $K = \{0, 1, a, b\}$ um corpo. Construa as tábuas de adição e da multiplicação desse corpo.

Sugestão: Comece com a tábua da multiplicação; depois mostre que $a + b = 1$, $1 + a = b$, etc.

40. Sejam A e B anéis com unidade. Ache os divisores próprios de zero de AxB bem como os elementos inversíveis deste anel. Pode AxB (produto direto) ser um corpo?

41. Dado um corpo K, um subconjunto $M \subset K$, $M \neq \phi$, se diz subcorpo de K se:

a) $1 \in M$

b) $a, b \in M \Rightarrow a - b \in M$ e

c) $a, b \in M$ e $b \neq 0 \Rightarrow a \cdot b^{-1} \in M$.

Mostre que M é fechado para a adição e a multiplicação de K.

Mostre que $(M, +, \cdot)$ é, também, um corpo.

42. Verifique se são subcorpos

a) $M = \{0, 1\}$ de um corpo K qualquer

b) $M = \{a + bi \mid a, b \in \mathbb{Q}\}$ do corpo C

c) $M = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$ do corpo $\mathbb{R}$.

43. Determinar quais dos seguintes subconjuntos de $\mathbb{R}$ são subcorpos:

a) $A = \{a + b\sqrt{2} \mid a \in \mathbb{Q} \text{ e } b \in \mathbb{Q}\}$

b) $B = \{a + b\sqrt[3]{2} \mid a \in \mathbb{Q} \text{ e } b \in \mathbb{Q}\}$

c) $C = \{a\sqrt{2} + b\sqrt{3} \mid a \in \mathbb{Q} \text{ e } b \in \mathbb{Q}\}$

d) $D = \{a + b\sqrt{2} \mid a \in \mathbb{Z} \text{ e } b \in \mathbb{Z}\}$

44. Se B e C são subcorpos de um corpo A, então $B \cap C$ é um subcorpo de A.

45. Prove que o único subcorpo de $\mathbb{Q}$ é o próprio $\mathbb{Q}$.

Prove que se K é subcorpo de Q então $K = \mathbb{Q}$.

46. Prove que $\mathbb{Q}$ é o "menor" subcorpo de $\mathbb{R}$.

Sugestão: Prove que se K é subcorpo de R então $\mathbb{Q} \subset K$.

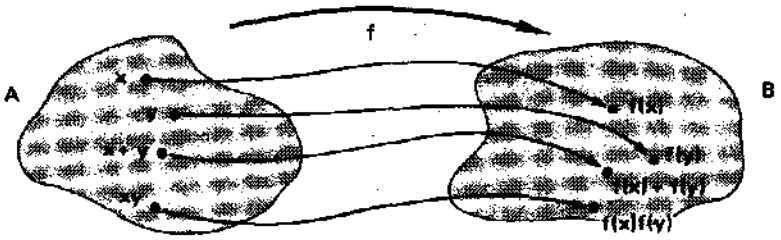
47. Verdadeiro ou Falso: Existem infinitos subcorpos de $\mathbb{R}$?

Dê uma justificativa razoável para a resposta.

§ 3º — HOMOMORFISMOS — ISOMORFISMOS

1. HOMOMORFISMOS

Sejam A e B anéis arbitrários. Dentre as aplicações existentes de A em B, têm importância destacada aquelas que "preservam" as leis de composição internas que fazem de A e B anéis, conforme os estamos considerando. O "preservar" aí significa aquilo que pode ser visualizado no diagrama e que traduziremos na definição a seguir:



Definição 9: Sejam A e B dois anéis. Uma aplicação f: A ⟶ B é chamada *homomorfismo* de A em B se as seguintes condições se verificam:

(i) $(\forall\ x, y)(x, y \in A \implies f(x + y) = f(x) + f(y))$

(ii) $(\forall\ x, y)(x, y \in A \implies f(xy) = f(x)f(y))$.

Exemplo: Sejam A = ℤ e B = ℤxℤ (produto direto). A aplicação f: ℤ ⟶ ℤxℤ, dada por f(x) = (x, 0), ∀ x ∈ ℤ, é um homomorfismo de anéis porque

$f(x + y) = (x + y, 0) = (x, 0) + (y, 0) = f(x) + f(y)$ e

$f(xy) = (xy, 0) = (x, 0)(y, 0) = f(x)f(y)$

2. NÚCLEO DE UM HOMOMORFISMO

Definição 10: Dado um homomorfismo de anéis f: A ⟶ B, o *núcleo* de f é o subconjunto N(f) ⊂ A (também indicado por Ker(f)), definido da seguinte maneira:

$$N(f) = \{x \in A \mid f(x) = 0_B\}$$

Exemplo: Achemos o núcleo do homomorfismo que apareceu no item anterior: $N(f) = \{m \in \mathbb{Z} \mid (m, 0) = (0, 0)\}$. Logo: $m \in N(f) \iff m = 0$. Assim, $N(f) = \{0\}$.

3. PROPOSIÇÕES

Seja f: A ⟶ B um homomorfismo de anéis.

P_1) $f(0_A) = 0_B$, $f(-a) = -f(a)$, ∀ a ∈ A e $f(a - b) = f(a) - f(b)$, ∀ a, b ∈ A.

Demonstração: (A, +) e (B, +) são grupos e f: A ⟶ B é um homomorfismo de grupos. *Portanto a demonstração desses três fatos é a mesma já feita* para grupos. Fica como exercício. ■

Se f:A ⟶ B é um homomorfismo de anéis e f é aplicação injetora, dizemos que f é um *homomorfismo injetor* ou *monomorfismo* de anéis.

Por exemplo, o homomorfismo f: ℤ ⟶ ℤxℤ dado por f(x) = (x, 0) é injetor porque

$$f(x) = f(y) \implies (x, 0) = (y, 0) \implies x = y.$$

P_2) O homomorfismo de anéis f: A ⟶ B é injetor se, e somente se, $N(f) = \{0_A\}$.

Demonstração: (⟹) Seja $x \in N(f)$. Então $f(x) = 0_B = f(0_A)$. Sendo f injetora, segue disso que $x = 0_A$. Portanto $N(f) = \{0_A\}$.

(⟸) Suponhamos x, y ∈ A e f(x) = f(y). Então:

$f(x) = f(y) \implies f(x) - f(y) = 0_B \implies f(x - y) = 0_B \implies x - y = 0_A \implies x = y.$

Logo f é injetora. ■

Se f: A ⟶ B é um homomorfismo de anéis e se f é uma aplicação sobrejetora, damos o nome a f de *homomorfismo sobrejetor* ou *epimorfismo* de anéis.

Por exemplo, consideremos a aplicação f: ℤxℤ (produto direto) ⟶ ℤ dada por f(x, y) = x, ∀ (x, y) ∈ ℤxℤ, f é um homomorfismo de anéis porque

$$f((x, y) + (x', y')) = f(x + x', y + y') = x + x' = f(x, y) + f(x', y')$$

e

$$f((x, y)(x', y')) = f(xx', yy') = xx' = f(x, y)\,f(x', y')$$

Além disso, é também sobrejetor uma vez que, para todo a ∈ ℤ, tomando qualquer par (a, y), teremos f(a, y) = a.

P_3) Suponhamos f: A ⟶ B homomorfismo sobrejetor de anéis. Então: a) Se A possui unidade o mesmo acontece com B e a unidade deste anel é $1_B = f(1_A)$; (b) Se existe unidade em A e a ∈ A é inversível, então f(a) também é inversível e $f(a^{-1}) = (f(a))^{-1}$.

Demonstração: (a) Seja b um elemento qualquer de B. Então existe $a \in A$ de modo que $f(a) = b$. Daí

$$bf(1_A) = f(a)f(1_A) = f(a1_A) = f(a) = b$$

e, analogamente, $f(1_A)b = b$.

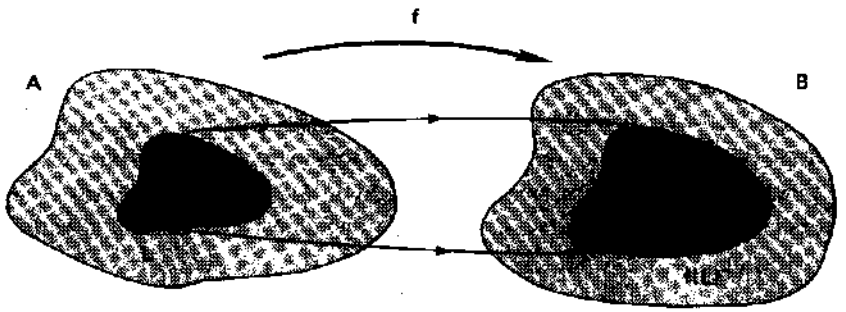
Logo $f(1_A) = 1_B$.

(b) $f(a)f(a^{-1}) = f(aa^{-1}) = f(1_A) = 1_B$, para todo $a \in A$. Do mesmo modo se verifica que $f(a^{-1})f(a) = 1_B$. Portanto $(f(a))^{-1} = f(a^{-1})$. Recomendamos ao leitor verificar onde usamos, na demonstração, a hipótese de que f é sobrejetora. ■

Nota: Se $f: A \longrightarrow B$ é um homomorfismo de anéis e L é um subanel de A, então f(L) também é um subanel de B. É claro que $f(L) \neq \phi$. Por outro lado f(L) é fechado tanto para a subtração como para a multiplicação de B porque, $\forall\ x, y \in L$:

$$f(x) - f(y) = f(x - y),\quad f(x)f(y) = f(xy),\quad \text{e}\quad x - y,\ xy \in L.$$

Logo um homomorfismo de anéis transforma os subanéis de A em subanéis de B. Em particular, se f for sobrejetor, f(A) = B.



4. ISOMORFISMOS DE ANÉIS

Tal como acontece para os grupos, de que já tratamos, há casos em que as diferenças entre dois anéis A e B, enquanto considerados como tal, são apenas formais. Os elementos de A e os de B têm, vamos dizer, "nomes" diferentes, pode acontecer o mesmo com relação às leis de composição internas envolvidas, mas ficam aí as diferenças sob o ponto de vista da definição de anel. Isso naturalmente pressupõe que os conjuntos A e B sejam equipotentes e, algèbricamente falando, a existência de um homomorfismo relacionando A e B. Nessas condições podemos considerar A e B "indistintos" como anéis.

Definição 11: Sejam A e B anéis quaisquer. Uma aplicação $f: A \longrightarrow B$ é chamada isomorfismo de A em B se

(i) f é bijetora

(ii) f é um homomorfismo de anéis, isto é:
$f(x + y) = f(x) + f(y)$ e $f(xy) = f(x)f(y)$, $\forall\ x, y \in A$.

Nota: Naturalmente todos os resultados válidos para homomorfismos de anéis também são válidos para isomorfismos. Além disso, pode-se provar (em demonstração análoga à que fizemos para grupos), que se $f: A \longrightarrow B$ é um isomorfismo de anéis, então $f^{-1}: B \longrightarrow A$ também é um isomorfismo de anéis. Deixamos proposto como exercício este resultado. Em razão desse fato é que dizemos que os anéis A e B são *isomorfos,* quando existe um isomorfismo relacionando os dois.

Exemplo: Sejam A e B anéis arbitrários. Indiquemos o zero do anel B simplesmente por 0. Sendo assim, se construirmos o produto direto AxB o subconjunto $A \times \{0\}$ é um subanel de AxB. De fato além de $A \times \{0\}$ ser um subconjunto não vazio temos

$(a, 0), (b, 0) \in A \times \{0\} \Longrightarrow (a, 0) - (b, 0) = (a - b, 0) \in A \times \{0\}$ e

$(a, 0)(b, 0) = (ab, 0) \in A \times \{0\}$.

Tal subanel é isomorfo ao anel A mediante a aplicação $f: A \longrightarrow A \times \{0\}$ dada por $f(x) = (x, 0)$, $\forall\ x \in A$. Verifiquemos.

- $f(x) = f(y) \Longrightarrow (x, 0) = (y, 0) \Longrightarrow x = y$. Logo f é injetora.
- Dado $(b, 0) \in A \times \{0\}$, é claro que tomando $b \in A$ teremos $f(b) = (b, 0)$. Isso mostra que f é sobrejetora.
- $\forall\ x, y \in A$, $f(x + y) = (x + y, 0) = (x, 0) + (y, 0) = f(x) + f(y)$
- $\forall\ x, y \in A$, $f(xy) = (xy, 0) = (x, 0) \cdot (y, 0) = f(x) \cdot f(y)$

Contra-exemplo. Vamos considerar agora dois anéis comutativos com unidade, ambos formados de quatro elementos mas, apesar disso tudo, não isomorfos. Tais anéis são $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ cujas tábuas (tábua da adição e tábua da multiplicação) vêm a seguir

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

e o anel A das funções de um conjunto $X = \{x, y\}$ de dois elementos no anel $Z_2 = \{0, 1\}$. Os elementos deste último são as funções *a, b, c* e *d* assim construidas

$$a:\begin{cases} x \longrightarrow 0 \\ y \longrightarrow 0 \end{cases}, \quad b:\begin{cases} x \longrightarrow 1 \\ y \longrightarrow 1 \end{cases}, \quad c:\begin{cases} x \longrightarrow 1 \\ y \longrightarrow 0 \end{cases} \quad \text{e} \quad d:\begin{cases} x \longrightarrow 0 \\ y \longrightarrow 1 \end{cases}$$

As tábuas da adição e da multiplicação desse anel de funções são

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

·	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	c	a
d	a	d	a	d

Para calcularmos $b + c$ e cd, por exemplo, procedemos assim

$$(b + c)(x) = b(x) + c(x) = 1 + 1 = 0$$
$$(b + c)(y) = b(y) + c(y) = 1 + 0 = 1$$

o que mostra que $b + c = d$: além disso

$$(cd)(x) = c(x)d(x) = 1 \cdot 0 = 0$$
$$(cd)(y) = c(y)d(y) = 0 \cdot 1 = 0$$

o que significa que $cd = a$.

Vejamos agora porque não são isomorfos esses anéis. Se existisse um isomorfismo $f: Z_4 \longrightarrow A$, teríamos $f(0) = a$ (zero de A) e $f(1) = b$ (unidade de A), devido às proposições P_1 e P_3 sobre homomorfismos, vistas no item anterior. Então haveria duas alternativas

$$f(2) = c \quad \text{e} \quad f(3) = d$$
ou
$$f(2) = d \quad \text{e} \quad f(3) = c.$$

Mostremos que nenhuma delas corresponde a isomorfismo. No primeiro caso, se f fosse isomorfismo, teríamos:

$f(2 \cdot 3) = f(2)f(3) \Longrightarrow f(2) = f(2)f(3) \Longrightarrow c = cd \Longrightarrow c = a$ (absurdo).

A segunda alternativa nos levaria também a uma contradição, como é óbvio.

Logo, entre esses dois anéis existe uma diferença que não é apenas formal ou de "nomes". Aliás, isso já poderia ser percebido, de vários modos, através das tábuas. Por exemplo, enquanto que na tábua da adição de A a diagonal principal é formada pela repetição do zero desse anel, o mesmo não acontece com a tábua da adição de Z_4. Sugerimos ao leitor procurar outras diferenças desse tipo.

Nota: Sejam A e B anéis. Suponhamos L um subanel de A. Se existe um homomorfismo injetor $f: A \longrightarrow B$ então f(L) é um subanel de B conforme vimos anteriormente. Daí $f|L : L \rightarrowtail f(L)$ é isomorfismo. Logo, existindo um isomorfismo injetor de A em B, o anel B contém uma "cópia" de cada um dos subanéis de A: para cada subanel L de A essa cópia é f (L).

5. CORPO DAS FRAÇÕES DE UM ANEL DE INTEGRIDADE
(EXEMPLO IMPORTANTE DE ISOMORFISMO DE ANÉIS)

Todo corpo, como já vimos, é um anel de integridade. Logo podemos dizer que todo corpo contém um subanel que é um anel de integridade: ele próprio. Nosso propósito agora é mostrar que, a menos de isomorfismos, todo anel de integridade é um subanel unitário de um certo corpo.

Seja A um anel de integridade. No conjunto $A \times A^*$ consideremos a relação assim definida:

$$(a, b) \sim (c, d) \iff ad = bc$$

Não é difícil verificar que se trata de uma relação de equivalência. Mostremos que vale a propriedade transitiva. Consideremos (a, b), (c, d) e (e, f) em $A \times A^*$. Suponhamos que $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$. Então $ad = bc$ e $cf = de$. Multiplicando a primeira dessa igualdades por f e a segunda por b obtemos: $adf = bcf$ e $bcf = bde$. Donde $adf = bde$. Como $d \neq 0$, segue desta última igualdade que $af = be$ o que significa $(a, b) \sim (e, f)$.

Um elemento $\overline{(a, b)}$ do conjunto quociente $K = (A \times A^*)/\sim$ é indicado, neste caso, por $\frac{a}{b}$. Assim

$$K = \left\{ \frac{a}{b} \mid a \in A \text{ e } b \in A^* \right\}$$

Evidentemente

$$\frac{a}{b} = \frac{c}{d} \iff ad = bc.$$

Nosso objetivo é fazer de K um corpo. Inspirados no que foi feito no item 3 do parágrafo anterior definiremos

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{e} \quad \frac{a}{b}\,\frac{c}{d} = \frac{ac}{bd}$$

quaisquer que sejam $\frac{a}{b}$ e $\frac{c}{d}$ em K.

Pode-se provar que essas definições independem das particulares representações das classes de equivalências. Façamos isso quanto à multiplicação. Vamos supor $(a, b) \sim (m, n)$ e $(c, d) \sim (r, s)$ e provar que $\frac{a}{b}\,\frac{c}{d} = \frac{m}{n}\,\frac{r}{s}$.

Por hipótese $an = bm$ e $cs = dr$. Donde $ancs = bmdr$ ou $(ac)(ns) = (bd)(mr)$. Vale dizer: $(ac, bd) \sim (mr, ns)$ ou, o que é equivalente, $\frac{a}{b}\,\frac{c}{d} = \frac{m}{n}\,\frac{r}{s}$. É uma questão de pura rotina provar que $(K, +, \cdot)$ *é um corpo*. Destaquemos o seguinte:

- O zero desse corpo é o elemento $\frac{0}{1}$ (0 = zero de A; 1 = unidade de A);
- A unidade de K é $\frac{1}{1}$;
- Dado $\frac{a}{b} \in K$, $-\frac{a}{b} = \frac{-a}{b}$;
- Dado $\frac{a}{b} \in K$, se $\frac{a}{b} \neq \frac{0}{1}$ então $(\frac{a}{b})^{-1} = \frac{b}{a}$.

Mostraremos agora que A pode ser visto como um subanel unitário de K. Para tanto consideremos o seguinte subconjunto de K:

$$L = \{\frac{a}{1} \mid a \in A\}.$$

É claro que $L \neq \phi$. Por outro lado, tomando $\frac{a}{1}$ e $\frac{b}{1}$ em L, teremos

$$\frac{a}{1} - \frac{b}{1} = \frac{a-b}{1} \in L \quad \text{e} \quad \frac{a}{1}\,\frac{b}{1} = \frac{ab}{1} \in L.$$

Logo L é um subanel de K. É unitário pois $\frac{1}{1}$ é a unidade, tanto de K como de L. Podemos dizer, pois, que L é um anel de integridade.

Trataremos agora de relacionar A com L. Se indicarmos por x um elemento genérico de A, um elemento genérico de L será $\frac{x}{1}$. Logo, a correspondência natural entre A e L é dada por

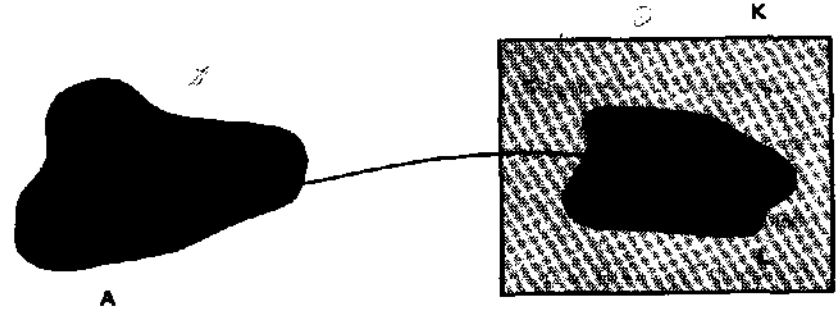
$$x \longmapsto \frac{x}{1}$$

Vamos chamar de f essa aplicação e mostrar que se trata de um isomorfismo.

- $f(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = f(a) + f(b)$, $\forall\ a, b \in A$;
- $f(ab) = \frac{ab}{1} = \frac{a}{1}\,\frac{b}{1} \Rightarrow f(a)f(b)$, $\forall\ a, b \in A$;
- $f(a) = f(b) \Longrightarrow \frac{a}{1} = \frac{b}{1} \Longrightarrow (a, 1) \sim (b, 1) \Longrightarrow a = b$.

- Dado $y = \frac{x}{1} \in L$, é claro que $x \in A$. Como $f(x) = y$, podemos dizer que f *é sobrejetora*.

Logo os anéis A e L podem ser vistos como o "mesmo" anel, naturalmente identificando cada elemento $x \in L$ com o seu correspondente $\frac{x}{1}$ no isomorfismo definido acima. Nessas condições é que podemos dizer que $A \subset K$ ou que A *é um subanel unitário de* K. L *é simplesmente uma "cópia" de* A.



Observemos que a construção do corpo dos racionais a partir do anel dos inteiros é um caso particular do que acabamos de ver.

EXERCÍCIOS

48. Verificar se a função $f: A \longrightarrow B$ é ou não é um homomorfismo do anel A no anel B, nos seguintes casos:
   1º) $A = \mathbb{Z}$, $B = \mathbb{Z}$, e $f(x) = x + 1$
   2º) $A = \mathbb{Z}$, $B = \mathbb{Z}$, $f(x) = 2x$
   3º) $A = \mathbb{Z}$, $B = \mathbb{Z} \times \mathbb{Z}$, $f(x) = (x, 0)$
   4º) $A = \mathbb{Z} \times \mathbb{Z}$, $B = \mathbb{Z}$, $f(x, y) = x$
   5º) $A = \mathbb{Z} \times \mathbb{Z} = B$, $f(x, y) = (y, x)$
   6º) $A = \mathbb{Z}$, $B = \mathbb{Z}_n$, $f(x) = \overline{x}$
   7º) $A = B = \mathbb{C}$ (conjunto dos complexos) e $f(a + bi) = a - bi$

49. Determinar os núcleos dos homomorfismos do exercício anterior.

50. Considere os anéis $\mathbb{Z}$ e $\mathbb{Z}\times\mathbb{Z}$ (produto direto). Verifique se são homomorfismos e determine o núcleo.

a) $f: \mathbb{Z}\times\mathbb{Z} \longrightarrow \mathbb{Z}\times\mathbb{Z}$ dado por $f(x, y) = (0, y)$

b) $f: \mathbb{Z}\times\mathbb{Z} \longrightarrow \mathbb{Z}$ dado por $f(x, y) = y$

c) $f: \mathbb{Z} \longrightarrow \mathbb{Z}\times\mathbb{Z}$ dado por $f(x) = (2x, 0)$

d) $f: \mathbb{Z}\times\mathbb{Z} \longrightarrow \mathbb{Z}\times\mathbb{Z}$ dado por $f(x, y) = (-y, -x)$

e) $f: \mathbb{Z} \longrightarrow \mathbb{Z}\times\mathbb{Z}$ dada por $f(x) = (0, x)$

51. Dê um exemplo de anéis A e B e um homomorfismo $f: A \longrightarrow B$ tal que $f(1_A) \neq 1_B$.

52. Mostre que $f: \mathbb{C} \longrightarrow M_2(\mathbb{R})$ dada por $f(a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, $\forall\ a, b \in \mathbb{R}$ é um monomorfismo de anéis.

Solução

Tomemos $z_1 = a + bi$ e $z_2 = c + di$ em $\mathbb{C}$:

Temos :

$$f(z_1 + z_2) = f((a + c) + (b + d)i) = \begin{pmatrix} a+c & -(b+d) \\ b+d & a+c \end{pmatrix} = \begin{pmatrix} a+c & -b-d \\ b+d & a+c \end{pmatrix} =$$

$$= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = f(z_1) + f(z_2)$$

$$f(z_1 \cdot z_2) = f((ac - bd) + (ad + bc)i) = \begin{pmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{pmatrix} =$$

$$= \begin{pmatrix} ac-bd & -ad-bc \\ ad+bc & ac-bd \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = f(z_1) \cdot f(z_2)$$

Observemos que f é um monomorfismo pois

$$f(z_1) = f(z_2) \Longrightarrow \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \Longrightarrow \begin{cases} a = c \\ b = d \end{cases} \Longrightarrow z_1 = z_2$$

53. Sejam os anéis $A = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Q}\}$ e $B = M_2(\mathbb{Q})$.

a) Mostre que $f: A \longrightarrow B$ dada por $f(a + b\sqrt{-2}) = \begin{pmatrix} a & -2b \\ b & a \end{pmatrix}$ é um homomorfismo.

b) f é um isomorfismo?

54. Considere os seguintes anéis: $(\mathbb{R}, +, \cdot)$ e $(\mathbb{R}, \oplus, \odot)$, sendo $a \oplus b = a + b + 1$ e $a \odot b = a + b + ab$. Mostre que $f: \mathbb{R} \longrightarrow \mathbb{R}$ dado por $f(x) = x - 1$, $\forall\ x \in \mathbb{R}$, é um isomorfismo de $(\mathbb{R}, +, \cdot)$ em $(\mathbb{R}, \oplus, \odot)$. Defina o isomorfismo inverso.

55. Seja A um anel. Para cada elemento inversível $a \in A$, seja $f_a: A \longrightarrow A$ a aplicação dada pela lei $f_a(x) = axa^{-1}$. Mostre que f_a é um isomorfismo e dê uma fórmula para $f_a \circ f_b$.

56. Seja $f: A \longrightarrow B$ um isomorfismo de anéis. Mostre que:

A) se $a \in A$ é um elemento idempotente, então $f(a)$ também o é;

B) se $a \in A$ é nilpotente, então $f(a) \in B$ também o é;

C) se A possui unidade, $a \in A$ e $\exists\ b, c \in A$ $(b, c \notin U(A))$ tais que $a = b \cdot c$, então $f(a) \in B$ pode também ser decomposto em dois fatores de B, ambos não inversíveis.

57. Mostre que nenhuma aplicação $f: A \longrightarrow B$, onde $A = \{x + y\sqrt{2} \mid x, y \in \mathbb{Q}\}$ $B = \{x + y\sqrt{3} \mid x, y \in \mathbb{Q}\}$ é isomorfismo.

Sugestão: Observe que se f fosse um isomorfismo de A em B, então $f(\sqrt{2}) = a + b\sqrt{3}$. Calcule a seguir $f(2) = 2$ a partir de $f(\sqrt{2}) = a + b\sqrt{3}$.

58. Mostre que se f é um isomorfismo do anel $A = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ nele próprio, então $f(\sqrt{2}) = +\sqrt{2}$ ou $f(\sqrt{2}) = -\sqrt{2}$.

59. Mostre que se $f: \mathbb{Z} \longrightarrow \mathbb{Z}$ é um isomorfismo de anéis, então f é a aplicação idêntica de $\mathbb{Z}$.

Sugestão: Observe que $f(\pm 1) = \pm 1$ e que $\forall\ m \in \mathbb{Z}^* \Longrightarrow m = (\pm 1) + \ldots + (\pm 1)$.

60. Mostre que se $f: \mathbb{Q} \longrightarrow \mathbb{Q}$ é um isomorfismo de anéis, então f é a aplicação idêntica de $\mathbb{Q}$.

Sugestão: Observe que $f(1) = 1 = (\frac{1}{n} + \frac{1}{n} + \ldots + \frac{1}{n})$, n vezes, $\forall\ n \in \mathbb{N}^*$.

A partir disto calcule $f(\frac{1}{n})$.

61. Calcular todos os homomorfismos de $\mathbb{Z}$ em $\mathbb{Z}$.

Solução

Seja $f: \mathbb{Z} \longrightarrow \mathbb{Z}$ um homomorfismo tal que $f(1) = k$.

Provemos que $f(x) = kx$ para todo $x \in \mathbb{Z}$:

1º) $f(0) = 0 = k \cdot 0$.

2º) Se $f(n) = kn$, com $n \in \mathbb{N}$, então :

$f(n + 1) = f(n) + f(1) = kn + k = k(n + 1)$

portanto, por indução, a tese esta provada para todo $x \in \mathbb{N}$.

3º) Se $x \in \mathbb{Z}$, então $x = -|x|$ e $|x| \in \mathbb{Z}_+$, então :

$f(x) = f(-|x|) = -f(|x|) = -k|x| = k(-|x|) = kx$

Tendo provado que f é uma função linear de x, determinemos agora o valor de k
Como $f(x \cdot y) = f(x) \cdot f(y)$ para todos $x, y \in \mathbb{Z}$, temos:

$$k(xy) = (kx) \cdot (ky) \quad \forall \quad x, y \in \mathbb{Z}$$

e daí:

$$k = k^2 \therefore k = 0 \text{ ou } k = 1.$$

Conclusão: há apenas dois homomorfismos do anel Z nele próprio: $f(x) = x$ e $f(x) = 0$.

62. Calcular todos os homomorfismos de $\mathbb{Z} \times \mathbb{Z}$ em $\mathbb{Z}$.

63. Determinar todos os homomorfismos do anel $\mathbb{Z}$ no anel $\mathbb{Z} \times \mathbb{Z}$.

64. Seja $f: \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ dada por $f(x, y) = (mx + ny, px + qy)$.

a) Calcular m, n, p, q de modo que f seja um homomorfismo do anel $\mathbb{Z} \times \mathbb{Z}$ nele mesmo;
b) Em quais desses casos f é um automorfismo ?

65. Ache todos os homomorfismos de $\mathbb{Z}$ em $\mathbb{Z}_4$.

Sugestão: Considere as imagens possíveis de $1 \in \mathbb{Z}$ por um homorfismo $f: \mathbb{Z} \longrightarrow \mathbb{Z}_4$.

66. Ache todos os homomorfismos de $\mathbb{Z}$ em $\mathbb{Z}_6$.

§ 4º — IDEAIS

1. IDEAIS NUM ANEL COMUTATIVO

Neste parágrafo e todas as vêzes em que intervier o conceito de "ideal", a ser definido a seguir, estaremos considerando apenas anéis comutativos. A noção de ideal é das mais importantes em Álgebra: grande parte da teoria dos anéis comutativos, como o leitor poderá observar já a partir dos próximos itens e grande parte das aplicações dessa teoria, giram em torno de tal conceito. Vejamos sua definição.

Definição 12: Seja A um anel comutativo. Dizemos que um subconjunto $I \subset A$, $I \neq \phi$, é um *ideal* em A se, e somente se,

(i) $(\forall x, y)\ (x, y \in I \implies x - y \in I)$

(ii) $(\forall a, x)\ (a \in A \text{ e } x \in I \implies ax \in I)$.

Exemplos

1) No anel $\mathbb{Z}$ dos inteiros todos os subconjuntos $n\mathbb{Z} = \{nq \mid q \in \mathbb{Z}\}$, onde n é um número inteiro dado, são ideais. De fato:

- $0 \in n\mathbb{Z}$ uma vez que $0 = n0$.
- $nq_1 - nq_2 = n(q_1 - q_2) \in n\mathbb{Z}$.
- $a(nq) = n(aq) \in n\mathbb{Z}$, $\forall\ a \in \mathbb{Z}$.

É possível, por outro lado, provar que se I é um ideal em $\mathbb{Z}$, então existe $n \in \mathbb{Z}$ de tal modo que $I = n\mathbb{Z}$. Isto será feito no item seguinte.

2) Para todo anel A são ideais em A, como é fácil verificar, os subconjuntos $\{0\}$ e A. São os chamados *ideais triviais* de A.

3) Seja A o anel das funções de $\mathbb{R}$ em $\mathbb{R}$. Mostremos que é ideal em A o seguinte subconjunto de A: $I = \{f: \mathbb{R} \longrightarrow \mathbb{R} \mid f(1) = 0\}$.

- A função nula pertence a I pois evidentemente se anula no ponto 1.
- Sejam f e g funções de I. Então $f(1) = g(1) = 0$. Donde $(f - g)(1) = f(1) - g(1) = 0 - 0 = 0$. Ou seja, $f - g \in I$.
- Seja f uma função de I e h uma função de A. Então $(hf)(1) = h(1)f(1) = h(1) \cdot 0 = 0$. Logo $hf \in I$.

4) Seja $f: A \longrightarrow B$ um homomorfismo de anéis. Mostremos que o núcleo $N(f)$ é um ideal em A. Lembremos que $N(f) = \{x \in A \mid f(x) = 0 \text{ (zero de B)}\}$.

- Como $f(0_A) = 0_B$, então $0_A \in N(f)$
- Suponhamos $x, y \in N(f)$. Então $f(x) = f(y) = 0$. Daí $f(x-y) = f(x) - f(y) = 0 - 0 = 0$. Donde $x - y \in N(f)$.
- Suponhamos $x \in N(f)$ e $a \in A$. Então $f(ax) = f(a)f(x) = f(a)0 = 0$ o que quer dizer que $ax \in N(f)$.

Nota: É claro que todo ideal num anel A é um subanel de A. Contudo a recíproca não vale. Por exemplo, $\mathbb{Z}$ é um subanel de $\mathbb{Q}$ mas não é um ideal em $\mathbb{Q}$. Basta notar que $1 \in \mathbb{Z}$, $\frac{1}{2} \in \mathbb{Q}$, mas $\frac{1}{2} \cdot 1 = \frac{1}{2} \notin \mathbb{Z}$.

Proposição 5: Seja I um ideal num anel comutativo A. Então:

(a) $0 \in I$ (isto é, o zero de A pertence a I);

(b) $(\forall a)(a \in I \Longrightarrow -a \in I)$;

(c) $(\forall a, b)(a, b \in I \Longrightarrow a + b \in I)$

(d) Se o anel A possui unidade e se existe um elemento inversível $u \in A$ tal que $u \in I$, então $I = A$.

Demonstração:

(a) $I \neq \phi \Longrightarrow \exists\ a \in I \Longrightarrow a - a \in I \Longrightarrow 0 \in I$.

(b) $a \in I$, por hipótese, e $0 \in I$, devido à parte (a); logo, $0 - a \in I$, isto é, $-a \in I$.

(c) Como a e b pertencem a I, por hipótese, então a e $-b$ pertencem a I; logo, $a - (-b) \in I$. Donde $a + b \in I$.

(d) Seja $a \in I$. Podemos escrever $a = a \cdot 1$. Como u é inversível, existe um elemento $v \in A$ de maneira que $uv = 1$. Donde $a = (au)v$ e usando a condição (ii) da definição, temos:

$$a \in A \text{ e } u \in I \Longrightarrow au \in I$$
$$au \in I \text{ e } v \in A \Longrightarrow (au)v \in I$$

e podemos concluir que $a \in I$. Provamos assim que $A \subset I$. Como obviamente $I \subset A$, temos então a igualdade proposta. ■

2. IDEAIS GERADOS — IDEAIS PRINCIPAIS

Seja A um anel comutativo. Tomemos $a_1, a_2, \ldots, a_n \in A$ $(n \geq 1)$. Indiquemos por $\langle a_1, a_2, \ldots, a_n \rangle$ o seguinte subconjunto de A:

$$\langle a_1, a_2, \ldots, a_n \rangle = \{x_1a_1 + x_2a_2 + \ldots + x_na_n \mid x_1, x_2, \ldots, x_n \in A\}$$

Tal subconjunto é um ideal em A. Verifiquemos:

- $0 = 0a_1 + 0a_2 + \ldots + 0a_n \Longrightarrow 0 \in \langle a_1, a_2, \ldots, a_n \rangle$.

- $r, s \in \langle a_1, a_2, \ldots, a_n \rangle \Longrightarrow \begin{cases} \exists\ x_1, \ldots, x_n \in A \mid r = x_1a_1 + \ldots + x_na_n \\ \exists\ y_1, \ldots, y_n \in A \mid s = y_1a_1 + \ldots + y_na_n \end{cases}$

Daí

$$r - s = (x_1 - y_1)a_1 + \ldots + (x_n - y_n)a_n \in \langle a_1, a_2, \ldots, a_n \rangle.$$

- Deixamos como exercício a verificação que falta fazer.

Definição 13: O ideal $\langle a_1, a_2, \ldots, a_n \rangle$ obtido segundo as considerações acima é chamado *ideal gerado* por $a_1, \ldots, a_n$. Um ideal gerado por um só elemento $a \in A$ recebe o nome de *ideal principal* gerado por a. Neste caso, além da notação $\langle a \rangle$, também é comum a seguinte: aA. (Esta última já foi usada, o leitor deve se lembrar, para indicar os ideais em $\mathbb{Z}$.) Se todos os ideais de um anel de integridade são principais, então este anel é chamado de *anel principal*.

Exemplo importante de anel principal: Afirmamos no item anterior que todo ideal em $\mathbb{Z}$ é do tipo $n\mathbb{Z}$, para um certo n natural conveniente. Justifiquemos essa afirmação.

Justificação: Seja I um ideal em $\mathbb{Z}$. Se I consta apenas do elemento zero de $\mathbb{Z}$, ou seja, $I = \{0\}$, é claro que I é principal pois $\langle 0 \rangle = \{0\}$.

Suponhamos $I \neq \{0\}$. Seja então b o menor dos elementos de I dentre os que são estritamente positivos. (O fato "$x \in I \Longrightarrow -x \in I$" nos garante, neste caso, a existência de elementos estritamente positivos em I.). Dado, pois, um elemento qualquer $a \in I$ sabemos que existem $q, r \in \mathbb{Z}$ de maneira que $a = bq + r$ $(0 \leq r < b)$. Daí

$$r = a - bq$$

que acarreta que $r \in I$, já que $a, b \in I$. Como b é o menor elemento estritamente positivo de I, não é possível $0 < r < b$; portanto, $r = 0$ e daí $a = bq$, ou seja $a \in \langle b \rangle$. Com isso provamos que $I \subset \langle b \rangle$. Como naturalmente $\langle b \rangle \subset I$, pois $b \in I$, então temos a igualdade $I = \langle b \rangle$ que vem provar nossa afirmação. ■

Proposição 6: Seja A um anel comutativo com unidade. Então: A é um corpo se, e somente se, os únicos ideais em A são os triviais.

Demonstração: $(\Longrightarrow)$ Seja I um ideal em A diferente do ideal nulo, isto é, $I \neq \langle 0 \rangle$. Então existe um elemento $a \in I$ tal que $a \neq 0$. Como A é um corpo, a é inversível e, pela proposição 5 - d, $I = A$.

$(\Longleftarrow)$ Tomemos $a \in A$, $a \neq 0$, e consideremos o ideal $I = \langle a \rangle$. Levando em conta a hipótese, podemos dizer que $\langle a \rangle = A$. Logo todo elemento de A pode ser escrito assim: xa, com $x \in A$. Em particular, existe $x_0 \in A$ tal que $1 = x_0a$ o que vem mostrar que a é inversível. Quer dizer, a é inversível qualquer que seja $a \in A$, $a \neq 0$. Logo A é um corpo. ■

3. OPERAÇÕES COM IDEAIS

a) Intersecção

Dados os ideais I e J num anel comutativo A pode-se mostrar que $I \cap J$ também é um ideal em A. De fato

- $0 \in I$ e $0 \in J \Longrightarrow 0 \in I \cap J$
- $x, y \in I \cap J \Longrightarrow (x, y \in I$ e $x, y \in J) \Longrightarrow (x - y \in I$ e $x - y \in J) \Longrightarrow$
  $\Longrightarrow x - y \in I \cap J$.
- $(x \in I \cap J$ e $a \in A) \Longrightarrow (x \in I, x \in J$ e $a \in A) \Longrightarrow (ax \in I$ e $ax \in J)$
  $\Longrightarrow ax \in I \cap J$.

b) Adição

Se I e J são ideais em A, indicamos pela notação I + J o seguinte subconjunto de A:

$$I + J = \{x + y \mid x \in I \text{ e } y \in J\}.$$

Trata-se também de um ideal em A porque, além de não ser vazio:

(i) $r, s \in I + J \Longrightarrow (r = x_1 + y_1$ e $s = x_2 + y_2$ com $x_1, x_2 \in I$ e $y_1, y_2 \in J) \Longrightarrow$
$\Rightarrow r - s = (x_1 - x_2) + (y_1 - y_2) \in I + J$.

(ii) $(a \in I$ e $r = x + y \in I + J$ com $x \in I$ e $y \in J) \Longrightarrow ar = ax + ay \in I + J$.

O ideal I + J é chamado *ideal soma* de I com J. É claro que $I + J = J + I$, $I \subset I + J$ e $J \subset I + J$.

Proposição 7: Sejam I e J ideais num anel comutativo A. Então:

(a) $I \cap J$ é o maior ideal contido em I e em J;

(b) I + J é o menor ideal que contém I e J.

Demonstração: Naturalmente o "maior" e o "menor" que figuram no enunciado referem-se à relação de ordem "inclusão".

(a) Seja L um ideal em A tal que $L \subset I$ e $L \subset J$. Então $L \subset I \cap J$.

(b) Seja L um ideal em A tal que $I \subset L$ e $J \subset L$. Então: $r \in I + J \Longrightarrow$
$\Rightarrow (\exists x \in I$ e $\exists y \in J \mid r = x + y) \Longrightarrow r \in L$ (pois "$x, y \in L \Longrightarrow x + y \in L$"). Logo $I + J \subset L$. ■

4. IDEAIS PRIMOS E MAXIMAIS

Definição 14: Seja P um ideal num anel comutativo A. Dizemos que P é um *ideal primo* se $P \neq A$ e se é verdadeira a seguinte frase:

$$(\forall\, a, b \in A)(a, b \in P \Longrightarrow a \in P \text{ ou } b \in P)$$

produto

Exemplos

1) $\{0\}$ em $\mathbb{Z}$ é ideal primo pois $\{0\} \neq \mathbb{Z}$ e $ab \in \{0\} \Longrightarrow a \in \{0\}$ ou $b \in \{0\}$.

2) $2\mathbb{Z}$ em $\mathbb{Z}$ é ideal primo pois $2\mathbb{Z} \neq \mathbb{Z}$ e $ab \in 2\mathbb{Z} \Longrightarrow 2 \mid ab \Longrightarrow 2 \mid a$ ou $2 \mid b$
$\Longrightarrow a \in 2\mathbb{Z}$ ou $b \in 2\mathbb{Z}$

3) No anel $\mathbb{Z}x\mathbb{Z}$ (produto direto) o ideal $P = \{0\}x\mathbb{Z}$ é primo porque, além de ser diferente do anel $\mathbb{Z}x\mathbb{Z}$, o que é óbvio, temos:
$(a, b)(c, d) \in \{0\}x\mathbb{Z} \Longrightarrow (ac, bd) \in \{0\}x\mathbb{Z} \Longrightarrow ac = 0 \Longrightarrow a = 0$ ou $c = 0 \Rightarrow$
$\Rightarrow (a, b) \in \{0\}x\mathbb{Z}$ ou $(c, d) \in \{0\}x\mathbb{Z}$.

Definição 15: Um *ideal maximal* num anel comutativo A é um ideal M, $M \neq A$, com a seguinte propriedade: o único ideal em A que contém M, e é diferente de M, é o próprio anel A. Quer dizer, M é um elemento maximal, em relação à inclusão, no conjunto dos ideais em A que são diferentes de A.

Exemplos

1) $2\mathbb{Z}$ em $\mathbb{Z}$ é ideal maximal pois $2\mathbb{Z} \subsetneq \mathbb{Z}$ e se J é ideal em $\mathbb{Z}$ e $J \supsetneq 2\mathbb{Z}$ então $1 \in J$ e $J = \mathbb{Z}$.

2) No anel $A = \mathbb{Z}x\mathbb{Z}$ (produto direto) é maximal o ideal $M = \mathbb{Z}x2\mathbb{Z}$.

De fato, seja J um ideal em $\mathbb{Z}x\mathbb{Z}$ tal que $M \subsetneq J$. Então existe $(a, b) \in J$ de maneira que $(a, b) \notin M$. Isto significa que $b = 2q + 1$ (número impar). Como $(a - 1, 2q) \in J$, pois se trata de um elemento de M, então

$$(a, 2q + 1) - (a - 1, 2q) = (1, 1) \in J$$

Pertencendo a unidade de A ao ideal J vale a igualdade J = A. Assim o único ideal em A, estritamente maior que M, é A.

Proposição 8: Seja A um anel comutativo com unidade. Então todo ideal maximal em A é primo.

Demonstração: Seja M um ideal maximal e suponhamos $ab \in M$ e $a \notin M$. Consideremos o ideal $< a > + M$ em A que indicaremos apenas, como é costume neste tipo de soma, por $< a, M >$. Sendo assim $a \in < a, M >$ e $M \subset < a, M >$. Como porém $a \notin M$, temos então $M \subsetneq < a, M >$. Do fato de M ser maximal resulta então que $< a, M > = A$. Isto significa que todo elemento de A pode ser representado assim: $xa + m$, com $x \in A$ e $m \in M$. Em particular, existe $x_0 \in A$ e existe $m_0 \in M$ de tal maneira que $1 = x_0 a + m_0$. Portanto

$$b = x_0(ab) + bm_0$$

que mostra que $b \in M$, pois, tanto ab como m_0 estão em M. ■

EXERCÍCIOS

67. Verifique se são ideais:

a) $\{\overline{0}, \overline{2}, \overline{4}\}$ no anel $\mathbb{Z}_6$;

b) $m\mathbb{Z}$ no anel $\mathbb{Z}$;

c) $m\mathbb{Z} \times n\mathbb{Z}$ no anel $\mathbb{Z}\times\mathbb{Z}$;

d) $\{x \in \mathbb{Z} \mid \text{mdc } (x, 5) = 1\}$ no anel $\mathbb{Z}$;

e) $\{x \in \mathbb{Z} \mid 9 \text{ divide } 21x\}$ no anel $\mathbb{Z}$;

f) $\{x \in \mathbb{Z} \mid x \text{ divide } 24\}$ no anel $\mathbb{Z}$;

g) $\{x \in \mathbb{Z} \mid 6 \text{ divide } x \text{ e } 24 \text{ divide } x^2\}$ no anel $\mathbb{Z}$;

h) $\mathbb{Z}$ no anel $(\mathbb{Q}, \oplus, \odot)$ onde $a \oplus b = a + b - 1$ e $a \odot b = a + b - ab$ para todo $a, b \in \mathbb{Q}$;

i) $2\mathbb{Z}$ no anel $(\mathbb{Z}, +, \cdot)$ onde a adição é a usual e $a \cdot b = 0$ para todo $a, b \in \mathbb{Z}$;

j) $\{f: \mathbb{R} \longrightarrow \mathbb{R} \mid f(0) = 0\}$ no anel $\mathbb{R}^{\mathbb{R}}$;

68. Sendo A um anel (eventualmente não comutativo), dizemos que $I \subset A$ e $I \neq \emptyset$ é um *ideal à esquerda* em A se, e somente se:

$$(\forall x, y)\,(x \in I \text{ e } y \in I \Longrightarrow x - y \in I) \qquad (\forall x, z)\,(x \in I \text{ e } z \in A \Longrightarrow xz \in I)$$

Verificar se são ideais à esquerda em $M_2(\mathbb{R})$:

a) $L_1 = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$

b) $L_2 = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}$

c) $L_3 = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$

d) $L_4 = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$

69. Mostre que é um ideal em A o conjunto dos seus elementos nilpotentes.

Sugestão: Para mostrar que esse conjunto é fechado para a subtração, tomando x e y nilpotentes e tais que: $x^r = y^s = 0$, considere $(x + y)^{r+s}$.

70. Descrever os seguintes ideais principais:

a) $\langle \overline{2} \rangle$ em $\mathbb{Z}_6$

b) $\langle -5 \rangle$ em $\mathbb{Z}$

c) $\left\langle \frac{2}{7} \right\rangle$ em $\mathbb{Q}$

d) $\langle \sqrt{2} \rangle$ em $\mathbb{R}$

e) $\langle \overline{3} \rangle$ em $\mathbb{Z}_8$

f) $\langle 2 \rangle$ em $2\mathbb{Z}$

g) $\left\langle -\frac{3}{5} \right\rangle$ em $\mathbb{R}$

h) $\langle 1 - i \rangle$ em $\mathbb{C}$

71. Determinar todos os ideais de $\mathbb{Z}_8$.

72. Mostre que todos os ideais de um anel $\mathbb{Z}_m$ são principais.

73. a) Seja I um ideal do anel comutativo A. Provar que $J = \{x \in A \mid x \cdot i = 0, \forall\, i \in I\}$ é um ideal de A.

b) Determinar J no caso $A = \mathbb{Z}_{16}$ e $I = \langle 2 \rangle$.

74. Seja A um anel comutativo. Dados $a \in A$ e $b \in A$, dizemos que "a é associado de b" quando $a \mid b$ e $b \mid a$.

a) Provar que "a é associado de b", equivale a "os ideais $\langle a \rangle$ e $\langle b \rangle$ são iguais".

b) Quais são os elementos associados de 5 no anel $\mathbb{Z}$?

75. Sejam a, b e c elementos do anel de integridade $\mathbb{Z}$. Mostre que se $a = bc$ e $b \neq \pm a$, então $\langle a \rangle \subset \langle b \rangle$.

76. Sejam $I = \langle a \rangle$ e $J = \langle b \rangle$ ideais num anel A. Mostre $I \cdot J = \{xy \mid x \in I \text{ e } y \in J\}$ é um ideal em A e $I \cdot J = \langle ab \rangle$.

77. Sejam I e J dois ideais do anel A. Mostrar que se $I \cap J = \{0\}$ então $xy = 0$ para todo $x \in I$ e $y \in J$.

78. Se (I_r) é uma família de ideais, mostre que $\bigcap_r I_r$ é um ideal.

79. a) Dê um exemplo de dois ideais I e J num anel A de modo que $I \cup J$ não é ideal de A.

b) Se $I_1 \subset I_2 \subset I_3 \ldots$ é uma seqüência de ideais em A, mostre que $\bigcup_r I_r$ é um ideal de A.

80. Sejam $I = \langle x \rangle$ e $J = \langle y \rangle$ dois ideais de $\mathbb{Z}$. Mostrar que $I + J = \langle \text{mdc } (x, y) \rangle$ e que $I \cap J = \langle \text{mmc } (x, y) \rangle$; em seguida determinar $\langle 12 \rangle + \langle 21 \rangle$ e $\langle 12 \rangle \cap \langle 21 \rangle$

Solução

1º) Lembremos que m é mmc (a, b) se, e somente se, $a \mid m$, $b \mid m$; $a \mid m'$ e $b \mid m' \Rightarrow m \mid m'$; $m \geqslant 0$.

Provemos que $\langle a \rangle \cap \langle b \rangle = \langle m \rangle$. Sendo x um elemento qualquer de Z, temos:

$$x \in \langle a \rangle \cap \langle b \rangle \iff \left\{ \begin{matrix} x \in \langle a \rangle \iff a \mid x \\ x \in \langle b \rangle \iff b \mid x \end{matrix} \right\} \iff m \mid x \iff x \in \langle m \rangle$$

portanto, $\langle a \rangle \cap \langle b \rangle \subset \langle m \rangle$

2º) Lembremos que d é um mdc (a, b) se, e somente se, $d \geqslant 0$; $d \mid a$, $d \mid b$; $d' \mid a$ e $d' \mid b \Rightarrow d' \mid d$. Provemos que $\langle a \rangle + \langle b \rangle = \langle d \rangle$. Para qualquer inteiro x temos:

$$x \in \langle a \rangle + \langle b \rangle \Longrightarrow \left\{ \begin{matrix} x = ra + sb \\ d \mid a \\ d \mid b \end{matrix} \right\} \Longrightarrow d \mid x \iff x \in \langle d \rangle$$

portanto, $\langle a \rangle + \langle b \rangle \subset \langle d \rangle$

Sendo $\langle a \rangle + \langle b \rangle$ um ideal em $\mathbb{Z}$, $\langle a \rangle + \langle b \rangle$ é um ideal principal. Seja d' um gerador de $\langle a \rangle + \langle b \rangle$. Temos :

$$\left. \begin{matrix} a = a + 0 \Longrightarrow a \in \langle a \rangle + \langle b \rangle \Longrightarrow d' \mid a \\ b = 0 + b \Longrightarrow b \in \langle a \rangle + \langle b \rangle \Longrightarrow d' \mid a \end{matrix} \right\} \Longrightarrow d' \mid d \Longrightarrow \langle d \rangle \subset \langle d' \rangle$$

$$\langle d \rangle \subset \langle a \rangle + \langle b \rangle$$

3º) Em conseqüência do exposto :

$<12> \cap <21> = <\text{mmc}(12, 21)> = <84>$

$<12> + <21> = <\text{mdc}(12, 21)> = <3>$

81. Sejam a, b e c elementos fixados de um anel A. Prove que
$<a, b, c> = \{ax + by + cz \mid x, y, z \in A\}$
é um ideal em A. Em seguida, determine $m \in \mathbb{Z}$ tal que $<12, 20, 28> = <m>$ no anel $\mathbb{Z}$.

82. Seja f um homomorfismo do anel A no anel A'. Mostre que se I e J são ideais em A, então $f(I + J) = f(I) + f(J)$.

83. Seja I um ideal no anel A e a um elemento fixo de A. Mostre que o conjunto $<I, a> = \{i + ra \mid i \in I \text{ e } r \in A\}$ é ideal em A.
Determine, no caso $A = \mathbb{Z}$, o ideal $<<4>, 6>$.

84. No anel $\mathbb{Z}$ considere o ideal $I = <3>$. Mostre que o único ideal em $\mathbb{Z}$ que contém I é o próprio $\mathbb{Z}$; generalize este resultado.

85. Sejam $a_1, a_2, \ldots, a_m \in A$. Supondo A um anel com unidade mostre que $<a_1, a_2, \ldots, a_m>$ é o menor ideal em A que contém $\{a_1, a_2, \ldots, a_m\}$.

86. Seja a um elemento idempotente de um anel A com unidade. Mostre que
$A = <a> + <1 - a>$ e que $<a> \cap <1 - a> = \{0\}$.

87. Mostre que um anel comutativo com unidade A é anel de integridade se, e somente se, $<0>$ é primo.

88. Dê exemplos de ideais primos e não maximais.

89. Seja $a \neq 0$ um número inteiro. Prove que $<a>$ é primo se, e somente se, a é primo.

90. Se I é um ideal no anel A e se P é um ideal primo em I, então P é um ideal em A. Prove.

91. Mostre que todo ideal primo $P \neq <0>$ em $\mathbb{Z}$ é maximal.

92. Mostre que é maximal em $A = \mathbb{R}^{\mathbb{R}}$ o ideal $M = \{f \in A \mid f(1) = 0\}$.

§ 5º — ANÉIS-QUOCIENTES

1. CONCEITO DE ANEL-QUOCIENTE

Seja I um ideal no anel comutativo A. Consideremos a relação $\sim$ sobre A assim definida:

$$\forall x, y \in A,\ x \sim y \iff x - y \in I$$

Trata-se de uma relação de equivalência sobre A pois

- $0 \in I \Rightarrow x - x \in I\ (\forall x \in A) \Rightarrow x \sim x\ (\forall x \in A)$
- $x \sim y \Rightarrow x - y \in I \Rightarrow -(x - y) \in I \Rightarrow y - x \in I \Rightarrow y \sim x$
- $x \sim y$ e $y \sim z \Rightarrow x - y \in I$ e $y - z \in I \Rightarrow (x - y) + (y - z) \in I \Rightarrow$
$\Rightarrow x - z \in I \Rightarrow x \sim z$.

O conjunto-quociente de A por I é indicado, neste caso, por A/I, notação que é mais sugestiva pois, na verdade, a relação é determinada pelo ideal considerado.

Proposição 9: Se, com respeito à relação introduzida acima, a classe de equivalência de um elemento $a \in A$ é indicada como de praxe por $\bar{a}$, então $\bar{a} = \{a + i \mid i \in I\}$.

Demonstração: Indiquemos provisoriamente por E o conjunto $\{a + i \mid i \in I\}$ e provemos que $\bar{a} \subset E$ e $E \subset \bar{a}$.

Seja $x \in A$. Então

$x \in \bar{a} \Rightarrow x \sim a \Rightarrow x - a \in I \Rightarrow (\exists\, i_1 \in I$ tal que $x - a = i_1) \Rightarrow (\exists\, i_1 \in I \mid x = a + i_1) \Rightarrow x \in E$. Donde $\bar{a} \subset E$.

Para demonstrar a inclusão contrária é só percorrer a seqüência de implicações acima no sentido contrário. ■

Notação: Com base no resultado anterior indicaremos por $a + I$ a classe de equivalência $\bar{a}$. $a + I = \bar{a}$ é chamada *classe lateral* determinada por a, módulo I, em A.

É bom frisar que: $a + I = b + I \iff a \sim b \iff a - b \in I$.

Adição em A/I

A frase $(a + I) + (b + I) = (a + b) + I$, $\forall\, a, b \in A$, define uma lei de composição interna em A/I. De fato, se $a + I = a' + I$ e $b + I = b' + I$, então $a - a' \in I$ e $b - b' \in I$. Daí $(a - a') + (b - b') = (a + b) - (a' + b') \in I$, vale dizer, $(a + b) + I = (a' + b') + I$.

Essa lei de composição interna é a adição em A/I.

Relativamente a essa adição, A/I é um grupo abeliano porque

- $(a+I)+[(b+I)+(c+I)]=(a+I)+[(b+c)+I]=[a+(b+c)]+I=[(a+b)+c]+I=$
  $=[(a+b)+I]+(c+I)=[(a+I)+(b+I)]+(c+I)$.
- A demonstração da comutativa fica como exercício.
- O elemento neutro é a classe $0+I=I$, ou seja, o próprio ideal I.
- Para cada classe $a \in I$ a classe $(-a)+I$ é o elemento oposto de $a+I$ pois
  $(a+I)+(-a+I)=(a-a)+I=0+I=I$

Logo $-(a+I)=(-a)+I$.

Multiplicação em A/I

A frase $(a+I)(b+I)=ab+I$, $\forall$ a, b $\in$ I, define uma lei de composição interna em A/I que será chamada de multiplicação. Verifiquemos tal afirmação:
$a+I=a'+I$ e $b+I=b'+I \Rightarrow a-a' \in I$ e $b-b' \in I$. Daí

$$b(a-a') \in I \text{ e } a'(b-b') \in I.$$

Logo

$$b(a-a')+a'(b-b')=ba-ba'+a'b-a'b'=ba-b'a' \in I.$$

Isto significa que $ba+I=b'a'+I$.

Essa multiplicação apresenta as seguintes propriedades:

a) associativa (exercício)

b) comutativa (exercício)

c) é distributiva em relação à adição pois

$(a+I)[(b+I)+(c+I)]=(a+I)[(b+c)+I]=[a(b+c)]+I=(ab+ac)+I=$
$=(ab+I)+(ac+I)=(a+I)(b+I)+(a+I)(c+I)$.

Além disso, se o anel A possui unidade, o anel A/I também possui: é a classe $1+I$, onde 1 indica a unidade do anel A.

Portanto, (A/I, +, .) é também um anel comutativo (com unidade se A for um anel com unidade).

Definição 16: Dado um anel comutativo A, se I é um ideal em A, o anel (A/I, +, .) introduzido segundo as considerações acima, recebe o nome de *anel quociente* de A por I.

2. O TEOREMA DO HOMOMORFISMO

Seja f: A $\longrightarrow$ B um homomorfismo sobrejetor de anéis. Se I indica o núcleo de f, então A/I e B são anéis isomorfos.

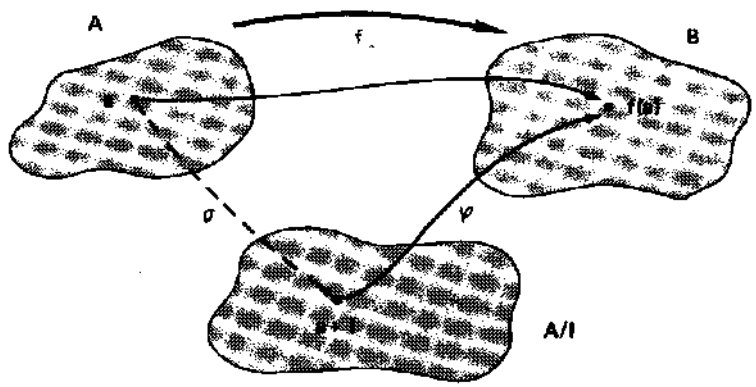
Demonstração: Já vimos, exemplo 4 do item 1 do parágrafo anterior, que o núcleo de um homomorfismo de anéis é um ideal. Logo tem sentido falar em A/I, conforme o enunciado.

Observemos que, dados a, a' $\in$ A,

$a+I=a'+I \Longrightarrow a-a' \in I \Longrightarrow f(a-a')=0$ (zero de B) $\Longrightarrow f(a)-f(a')=0 \Longrightarrow f(a)=f(a')$.

Isto significa que se associarmos a cada classe $x+I$ o elemento f(x) do anel B, fica definida uma aplicação φ de A/I em B. Mostremos que esta aplicação, dada por $\varphi(x+I)=f(x)$, $\forall$ x $\in$ A, é um isomorfismo de anéis.

- $\varphi((a+I)+(b+I))=\varphi((a+b)+I)=f(a+b)=f(a)+f(b)=\varphi(a+I)+\varphi(b+I)$.
- $\varphi((a+I)(b+I))=\varphi(ab+I)=f(ab)=f(a)f(b)=\varphi(a+I)\,\varphi(b+I)$.
- $f(a)=f(a') \Longrightarrow f(a)-f(a')=0 \Longrightarrow f(a-a')=0 \Longrightarrow a-a' \in I \Longrightarrow a+I=a'+I$.
- Dado b $\in$ B, existe a $\in$ A de modo que f(a) = b, pois f é sobrejetora. Considerando a classe $a+I$, vemos que $\varphi(a+I)=f(a)=b$. Logo φ é sobrejetora. ■

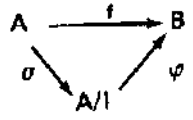


3. HOMOMORFISMO CANÔNICO

Observando o diagrama anterior percebe-se que a correspondência natural ligando os anéis A e A/I é a aplicação, que indicaremos por σ, definida da seguinte maneira: $\sigma(a)=a+I$, $\forall$ a $\in$ A. Na verdade trata-se de um homomorfismo sobrejetor o que, aliás, decorre da própria maneira como foram definidas as leis de composição internas em A/I. Verifiquemos.

- $\sigma(a+b)=(a+b)+I=(a+I)+(b+I)=\sigma(a)+\sigma(b)$
- $\sigma(ab)=(ab)+I=(a+I)(b+I)=\sigma(a)\,\sigma(b)$
- Por último, dada uma classe $x+I$, é claro que ela é imagem do elemento $x \in A$, pela aplicação σ. Logo σ é sobrejetora.

O homomorfismo acima definido é chamado *homomorfismo canônico* ou *homomorfismo natural* de A sobre A/I. Com ele podemos compor o seguinte diagrama de anéis e homomorfismos.



onde $\varphi \circ \sigma = f$.

Exemplo: Consideremos os anéis $A = \mathbb{Z}\times\mathbb{Z}$ (produto direto) e $B = \mathbb{Z}$. Já vimos anteriormente que a aplicação $f: \mathbb{Z}\times\mathbb{Z} \longrightarrow \mathbb{Z}$, dada por $f(x, y) = x$, $\forall\ (x, y) \in \mathbb{Z}\times\mathbb{Z}$, é um homomorfismo sobrejetor. Seja I o núcleo de f. Então

$$I = \{(x, y) \in \mathbb{Z}\times\mathbb{Z} \mid x = 0\} = \{(0, y) \mid y \in \mathbb{Z}\}$$

Portanto

$$(a, b) + I = (c, d) + I \iff (a, b) - (c, d) \in I \iff (a - c, b - d) \in I \iff a = c$$

Logo

$$(a, b) + I \neq (c, d) + I \iff a \neq c$$

Disto resulta que

$$A/I = \{(m, 0) + I \mid m \in \mathbb{Z}\}$$

Neste caso então

$$\sigma(a, b) = (a, 0) + I,\ \forall\ (a, b) \in \mathbb{Z}\times\mathbb{Z}$$

e

$$\varphi((m, 0) + I) = m,\ \forall\ m \in \mathbb{Z}$$

EXERCÍCIOS

93. Construir as tábuas do anel-quociente A/I nos seguintes casos:

a) $A = \mathbb{Z}$ e $I = \langle 2 \rangle$

b) $A = \mathbb{Z}$ e $I = \langle 4 \rangle$

c) $A = \mathbb{Z}$ e $I = \langle m \rangle$

d) A é um anel qualquer e $I = \langle 0 \rangle$

e) A é um anel qualquer e $I = A$

f) $A = \mathbb{Z}_2\times\mathbb{Z}$ e $I = \mathbb{Z}_2\times 2\mathbb{Z}$

g) $A = \mathbb{Z}_6$ e $I = \langle \overline{2} \rangle$

h) $A = \mathbb{Z}_8$ e $I = N(A)$ = conjuntos dos elementos nilpotentes de A.

94. Construa as tábuas dos seguintes anéis-quocientes:

$\mathbb{Z}_6 / (\overline{3})$ e $(\mathbb{Z}_2 \times \mathbb{Z}_3) / \langle \overline{1}, \overline{0} \rangle$

95. Provar que $2\mathbb{Z} \times 3\mathbb{Z}$ é subanel e um ideal $\mathbb{Z} \times \mathbb{Z}$. Determinar:

$(\mathbb{Z} \times \mathbb{Z}) / (2\mathbb{Z} \times 3\mathbb{Z})$.

96. Quais são os possíveis anéis-quocientes no corpo $\mathbb{R}$ dos números reais?

Sugestão: lembrar da proposição 6.

97. Mostre que se A possui unidade, então A/I também possui.

98. Mostre que $a + I \in A/I$ é inversível (supondo A com unidade) se, e somente se, $\exists\ r \in A$ de modo que $a \cdot r - 1 \in I$.

99. Dê um exemplo de um anel de integridade A e de um ideal I em A tal que A/I não é integridade.

Resolva o mesmo exercício quando A é um corpo.

100. Sendo I o ideal constituído pelos elementos nilpotentes de um anel A, mostre que I é o único elemento nilpotente de A/I.

Solução

Seja $\overline{a}$ um elemento nilpotente de A/I. Temos:

$$\exists\ n \in \mathbb{N} \mid (\overline{a})^n = \overline{0} \implies \overline{a^n} = \overline{0} \implies a^n \in I \implies \exists\ m \in \mathbb{N} \mid (a^n)^m = 0 \implies a^{nm} = 0$$

$$\implies a \in I \implies \overline{a} = a + I = I.$$

101. Dado o homomorfismo $f: \mathbb{Z} \longrightarrow \mathbb{Z}_4$ definido por $f(m) = \overline{m}$:

a) Construa o núcleo de f;

b) Determine o homomorfismo canônico de $\mathbb{Z}$ em $\mathbb{Z}/N(f)$.

102. Seja A um anel comutativo com unidade. Dado um ideal I em A prove que:

a) A/I é corpo $\iff$ I é maximal.

b) A/I é anel de integridade $\iff$ I é primo.

§ 6º — CARACTERÍSTICA DE UM ANEL

1. MÚLTIPLOS DE UM ELEMENTO DE UM ANEL

Seja $(A, +, .)$ um anel. Então $(A, +)$ é um grupo abeliano. Sendo assim já vimos no capítulo sobre grupos que se define múltiplo de um elemento $a \in A$, segundo um número inteiro m, da seguinte forma:

$$\left.\begin{array}{l} \text{se } m = 0,\ 0a = 0_A \\ \text{se } m \geqslant 0,\ ma = (m-1)a + a \\ \text{se } m < 0,\ ma = (-m)(-a) \end{array}\right\} \quad \text{(por recorrência)}$$

A partir dessa definição são válidas as seguintes propriedades:

(a) $(mn)a = m(na), \forall\ m, n \in \mathbb{Z}$ e $\forall\ a \in A$.

(b) $(m+n)a = ma + na, \forall\ m, n \in \mathbb{Z}$ e $\forall\ a \in A$.

(c) $(-m)a = m(-a) = -(ma), \forall\ m \in \mathbb{Z}$ e $\forall\ a \in A$.

Além dessas há uma outra, específica dos anéis com unidade, que teremos a ocasião de usar várias vezes neste parágrafo. É a proposição a seguir.

Proposição 9: Seja A um anel com unidade. Se m e n são dois números inteiros quaisquer, então $(mn)1_A = (m1_A)(n1_A)$.

Demonstração: Inicialmente suponhamos $n \geqslant 0$ e procedamos por indução neste caso. Se $n = 0$, então $(mn)1_A = 01_A = 0_A$ e $(m1_A)(n1_A) = (m1_A)0_A = 0_A$.

Seja $r \geqslant 0$ um número inteiro e admitamos que seja verdadeira a frase $(mr)1_A = (m1_A)(r1_A), \forall\ m \in \mathbb{Z}$. Daí:

$$[m(r+1)]1_A = (mr+m)1_A = (mr)1_A + m1_A = (m1_A)(r1_A) + m1_A = (m1_A)(r1_A + 1_A) =$$
$$= (m1_A)[(r+1)1_A].$$

Suponhamos agora $n < 0$. Então:

$$(m1_A)(n1_A) = (m1_A)[-((-n)1_A)] = -[(m1_A)((-n)1_A)] = -[(m(-n))1_A] = -[-(mn)1_A] =$$

2. CARACTERÍSTICA DE UM ANEL

Seja A um anel. Consideremos o seguinte subconjunto de $\mathbb{N}^*$:

$$S = \{n \in \mathbb{N}^* \mid na = 0 \text{ (zero de A)}, \forall\ a \in A\}.$$

Como S é um subconjunto de $\mathbb{N}^*$ há duas possibilidades apenas:

(i) $S = \phi$

Quando isto acontece, dizemos que o anel A tem *característica zero*.

Exemplo: Os anéis $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, têm característica zero porque, tomando $a = 1$, por exemplo, então $n \cdot 1 = n \neq 0, \forall\ n \in \mathbb{N}^*$, em qualquer um desses casos.

(ii) $S \neq \phi$

Neste caso, existe o mínimo de S (princípio do menor número inteiro). Se o mínimo de S é o número natural $h > 0$, dizemos que o anel A tem *característica* $h > 0$.

Exemplos:

1) Seja E um conjunto qualquer não vazio. Então o conjunto $A = \mathcal{P}(E)$ das partes de E é um anel em relação às seguintes leis de composição internas:

adição: $X + Y = \complement_{(X \cup Y)}^{(X \cap Y)}$

e multiplicação: $XY = X \cap Y$ (ver exercício 7 — Cap. III).

Observemos que o zero desse anel é o ϕ. Com efeito

$$X + \phi = \complement_{(X \cup \phi)}^{(X \cap \phi)} = \complement_{X}^{\phi} = X, \forall X \in A.$$

Por outro lado existem elementos em A diferentes de ϕ: pelo menos o conjunto E. Como $1E = E \neq \phi$, podemos dizer que a característica de A não é 1. Por último, observando que

$$X + X = \complement_{(X \cup X)}^{(X \cap X)} = \complement_{X}^{X} = \phi, \ \forall\ X \in A,$$

então a característica desse anel é exatamente dois.

2) Consideremos um anel qualquer $\mathbb{Z}_m$ de classes de restos e mostremos que sua característica é $m > 0$.

Dado $\bar{a} \in \mathbb{Z}_m$, temos

$$m\bar{a} = m(a\bar{1}) = (ma)\bar{1} = (am)\bar{1} = a(m\bar{1}) = a\bar{m} = a\bar{0} = \bar{0}.$$

Por outro lado não podemos ter $r\bar{a} = \bar{0}, \forall\ \bar{a} \in \mathbb{Z}_m$, com $0 < r < m$, pois isto implicaria que

$$r\bar{1} = \bar{r} = \bar{0}.$$

Daí então $\bar{r} = \bar{m}$ que equivale a $r \equiv m \pmod m$, ou seja, $r \equiv 0 \pmod m$. Logo $m \mid r$ o que é impossível.

Notação: indicaremos por c(A) a característica de um anel A.

Proposição 10: Seja A um anel com unidade. Então a característica de A é igual ao período da unidade (no grupo aditivo A).

Demonstração

1º caso: $c(A) = h > 0$.

Então decorre da própria definição de característica que $h1_A = 0$ (zero de A). Suponhamos que fosse possível o seguinte: $r1_A = 0$, com $0 < r < h$. Daí então, $\forall\ a \in A$,

$$ra = r(1_A a) = (r1_A)a = 0a = 0$$

o que não é possível dado que $0 < r < h$ e $c(A) = h$.

Logo $o(1_A) = h$.

2º caso: $c(A) = 0$. Fica como exercício a demonstração de que $o(1_A) = 0$. ■

Proposição 11: A característica de um anel de integridade A ou é zero ou é um número primo.

Demonstração: Seja A um anel de integridade cuja característica é diferente de zero. Seja $c(A) = h > 0$. Provemos que h é primo. Se não fosse existiriam dois números naturais não nulos r e s de maneira que

$$h = rs \quad e \quad 1 < r, s < h.$$

Nessas condições é claro que $r1_A \neq 0$ e $s1_A \neq 0$. Não obstante temos

$$(r1_A)(s1_A) = (rs)1_A = h1_A = 0$$

ou seja, $r1_A$ e $s1_A$ são divisores próprios do zero em A o que é absurdo. ■

Nota: Seja A um anel com unidade. Pelo que vimos até aqui é claro que o conceito de característica de um anel com unidade está intimamente ligado ao seguinte subconjunto de A: $\mathbb{Z}1_A = \{m1_A \mid m \in \mathbb{Z}\}$. Tal subconjunto é um subanel de A pois, além de não ser vazio (o elemento 1_A e o zero de A, por exemplo, pertencem a ele), temos o seguinte:

- $m1_A - n1_A = (m - n)1_A$ e
- $(m1_A)(n1_A) = (mn)1_A$, $\forall\ m, n \in \mathbb{Z}$.

Evidentemente $\mathbb{Z}1_A$ é um subanel unitário e comutativo de A. A proposição a seguir enfatiza ainda mais a conexão desse subanel com a característica de A.

Proposição 12: Seja A um anel com unidade. Se a característica de A é $h > 0$, então $\mathbb{Z}1_A$ é isomorfo a $\mathbb{Z}_h$. Se a característica de A é zero, então $\mathbb{Z}1_A$ é isomorfo a $\mathbb{Z}$.

Demonstração: Faremos a demonstração apenas no caso em que $c(A) = h > 0$. A cada elemento $\bar{r} \in \mathbb{Z}_h$ associemos o elemento $r1_A$. Mostremos que se trata de uma aplicação:

$\bar{r} = \bar{s} \Longrightarrow h \mid (r - s) \Longrightarrow r - s = ht\ (t \in \mathbb{Z}) \Longrightarrow (r - s)1_A = (ht)1_A = 0$ (zero de A) $\Longrightarrow r1_A = s1_A$.

Vamos dar o nome de f a essa aplicação e mostrar que f é um isomorfismo de $\mathbb{Z}_h$ em $\mathbb{Z}1_A$:

- $f(\bar{r} + \bar{s}) = (r + s)1_A = r1_A + s1_A = f(r) + f(s)$
- $f(\bar{r}\,\bar{s}) = (rs)1_A = (r1_A)(s1_A) = f(r)f(s)$
- $r1_A = s1_A \Longrightarrow (r - s)1_A = 0$ (zero de A) $\Longrightarrow h \mid (r - s) \Longrightarrow \bar{r} = \bar{s}$, o que mostra que f é injetora.
- é evidente que f é sobrejetora. ■

Interpretação: O significado da proposição acima é o seguinte: todo anel com unidade de característica zero contém uma "cópia" do anel $\mathbb{Z}$ e todo anel de característica $h > 0$ contém uma "cópia" do anel $\mathbb{Z}_h$. Em outras palavras, com as devidas identificações: todo anel de característica zero "contém" o anel $\mathbb{Z}$ e todo anel de característica $h > 0$ "contém" o anel $\mathbb{Z}_h$.

EXERCÍCIOS

103. Determinar as características dos seguintes anéis:

a) $\mathbb{Z}_3$ c) $\mathbb{Z} \times \mathbb{Z}$ e) $\mathbb{Z}_6 \times \mathbb{Z}_8$

b) $\mathbb{Z}$ d) $\mathbb{Z}_2 \times \mathbb{Z}$ f) $\mathbb{R}^{\mathbb{R}}$

104. Determinar a característica do anel das matrizes reais do tipo nxn sobre $\mathbb{R}$ e sobre $\mathbb{Z}_5$.

105. Sejam A e B dois anéis comutativos com elementos unidades. Demonstrar que a característica do anel-produto AxB é igual ao mmc das característica de A e de B.

106. Ache um anel de característica zero e um elemento a desse anel de forma que $na = 0$ para um certo $n \in \mathbb{N}^*$.

Sugestão: Tome, por exemplo, $A = \mathbb{Z}_2 \times \mathbb{Z}$.

107. Pode um anel finito ter característica zero ? Prove ou contra-exemplifique.

108. Dê um exemplo de um anel infinito cuja característica seja diferente de zero.

109. Pode um anel com unidade (diferente de zero) ter característica um? Por que?

110. Mostre que um anel de integridade com 4 elementos tem característica 2.

Sugestão: Raciocine em termos do período da unidade.

111. Seja A um anel cuja característica é um número natural $n > 0$ não primo. Mostre que A possui divisores próprios do zero.

112. Seja A um anel com unidade tal que $x^2 = x$, $\forall\, x \in A$. Mostre que $c(A) = 2$.

113. Seja A um anel e L um subanel de A. Mostre que $c(L) \leqslant c(A)$. Dê um exemplo de um anel A e um subanel L de A para os quais $c(L) < c(A)$.

114. Sejam A e B anéis isomorfos. Mostre que $c(A) = c(B)$.

115. Seja $f: A \longrightarrow B$ um epimorfismo de anéis. Mostre que $c(B) \geqslant c(A)$.

116. Mostre que o número de elementos de um corpo de característica p é uma potência de p.

117. Mostrar que se K é um corpo de característica $p > 0$, então $(x + y)^p = x^p + y^p$ para todos $x, y \in K$.

118. Seja K um corpo finito de característica $p > 0$: mostrar que a aplicação $f: K \longrightarrow K$ definida por $f(x) = x^p$ é um automorfismo de K. (*)

119. Chama-se *corpo primo* do corpo K a intersecção P de todos os subcorpos de K. Mostrar que o corpo primo P de um corpo K de característica p é isomorfo a $\mathbb{Z}_p$ (se $p > 1$) ou a $\mathbb{Q}$ (se $p = 0$).

120. Mostrar que o único automorfismo de um corpo primo é o automorfismo idêntico.

121. Mostrar que se P é o corpo primo de um corpo K de característica $p > 0$, então $a^p = a$, para todo $a \in P$.

(*) Um *automorfismo* de K é um isomorfismo de K no próprio K.

Capítulo IV

ANÉIS DE POLINÔMIOS

§ 1º — POLINÔMIOS SOBRE UM ANEL

1. SEQÜÊNCIAS

Conceito: No capítulo I, no parágrafo sobre Aplicações, chamamos de seqüência toda função definida no conjunto $\mathbb{N}^*$. Uma função $f: \mathbb{N} \longrightarrow A$ também é chamada *seqüência de elementos de A*. Neste capítulo, ao falarmos de seqüência, estaremos nos referindo a este último tipo. Consideraremos, ademais, apenas seqüências de elementos de um anel A.

Se a_i indica a imagem do elemento genérico $i \in \mathbb{N}$, através da aplicação (seqüência) f, tal seqüência é indicada por

$$f = (a_0, a_1, a_2, \ldots, a_i, \ldots)$$

Os elementos $a_0, a_1, a_2, \ldots, a_i, \ldots$ são chamados *termos* da seqüência. Muitas vezes usa-se a forma simplificada $f = (a_i)$ para indicar a seqüência $f = (a_0, a_1, a_2, \ldots, a_i, \ldots)$. É claro que $a_i \in A$ e $i \in \mathbb{N}$.

Igualdade: Sejam $f = (a_i)$ e $g = (b_i)$ seqüências de elementos de um anel A. Como se trata de funções (de $\mathbb{N}$ em A), então $f = g$ se, e somente se, $a_i = b_i$ para todo $i \in \mathbb{N}$.

Adição: Dadas duas seqüências $f = (a_i)$ e $g = (b_i)$ de elementos de um anel A, chama-se *soma* de f com g a seqüência $h = (c_i)$ tal que $c_i = a_i + b_i$ para todo $i \in \mathbb{N}$.

Exemplos

1º) Se $f = (a_i)$ tal que $a_i = 2i$ e $g = (b_i)$ tal que $b_i = i + 1$ são duas seqüências sobre $\mathbb{R}$, sua soma é $h = (c_i)$ onde:

$$c_i = a_i + b_i = 2i + (i + 1) = 3i + 1, \forall i \in \mathbb{N}$$

portanto:

$$h = (1, 4, 7, 10, 13, \ldots, 3i + 1, \ldots).$$

2º) Se $f = (1, 2, 4, 8, 16, 32, \ldots, 2^i, \ldots)$ e $g = (0, 0, 0, \ldots, 0, \ldots)$ então $h = f + g = (1, 2, 4, 8, \ldots, 2^i, \ldots)$.

3º) Se $f = (3, 2, 1, 0, 0, 0, \ldots, 0, \ldots)$ e $g = (4, 4, 4, 4, 0, 0, \ldots, 0, \ldots)$ então $h = f + g = (7, 6, 5, 4, 0, 0, \ldots, 0, \ldots)$.

Multiplicação: Dadas duas seqüências $f = (a_i)$ e $g = (b_j)$ sobre um anel A, chama-se *produto* de f por g a seqüência $h = (c_k)$ tal que:

$$c_0 = a_0 b_0$$

$$c_1 = a_0 b_1 + a_1 b_0$$

$$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$$

$$c_3 = a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0$$

. . . . . .

$$c_k = a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \ldots + a_k b_0$$

. . . . . .

isto é:

$$c_k = \sum_{i=0}^{k} a_i b_{k-i} \quad \text{para cada } k \in \mathbb{N}.$$

Exemplos

1º) Calcular os seis termos iniciais do produto das seqüências $f = (a_i)$ tal que $a_i = i$ e $g = (b_j)$ tal que $b_j = 2j$ sobre $\mathbb{R}$.

Temos:

$f = (0, 1, 2, 3, 4, 5, \ldots)$

$g = (0, 2, 4, 6, 8, 10, \ldots)$

Se $h = f \cdot g = (c_k)$, então:

$c_0 = 0 \cdot 0 = 0$

$c_1 = 0 \cdot 2 + 1 \cdot 0 = 0$

$c_2 = 0 \cdot 4 + 1 \cdot 2 + 2 \cdot 0 = 2$

$c_3 = 0 \cdot 6 + 1 \cdot 4 + 2 \cdot 2 + 3 \cdot 0 = 8$

$c_4 = 0 \cdot 8 + 1 \cdot 6 + 2 \cdot 4 + 3 \cdot 2 + 4 \cdot 0 = 20$

$c_5 = 0 \cdot 10 + 1 \cdot 8 + 2 \cdot 6 + 3 \cdot 4 + 4 \cdot 2 + 5 \cdot 0 = 40$

portanto:

$h = (0, 0, 2, 8, 20, 40, \ldots)$

2º) Calcular o produto das seqüências $f = (2, 1, 0, 0, \ldots, 0, \ldots)$ e $g = (3, 4, 5, 0, 0, \ldots, 0, \ldots)$ sobre $\mathbb{R}$.

Se $h = f \cdot g = (c_k)$, temos:

$c_0 = 2 \cdot 3 = 6$

$c_1 = 2 \cdot 4 + 1 \cdot 3 = 11$

$c_2 = 2 \cdot 5 + 1 \cdot 4 + 0 \cdot 3 = 14$

$c_4 = 2 \cdot 0 + 1 \cdot 5 + 0 \cdot 4 + 0 \cdot 3 = 5$

$c_5 = 2 \cdot 0 + 1 \cdot 0 + 0 \cdot 5 + 0 \cdot 4 + 0 \cdot 3 = 0$

$c_k = 0$ para todo $k \geq 5$

portanto:

$h = (6, 11, 14, 5, 0, \ldots, 0, \ldots)$

2. SEQÜÊNCIAS QUASE–NULAS OU POLINÔMIOS

Definição: Dado um anel A, uma seqüência $(a_0, a_1, a_2, \ldots)$ sobre A recebe o nome de *polinômio sobre A* se existe um índice $r \in \mathbb{N}$ tal que $a_m = 0$ para todo $m > r$.

Observando esta definição, notamos que uma seqüência (a_i) é um polinômio quando os termos que sucedem um certo a_r são todos nulos. A definição nada impõe para $a_0, a_1, a_2, \ldots, a_r$ que podem ser, alguns deles ou mesmo todos, iguais a zero. Daí se conclui que uma seqüência é um polinômio quando apresenta um número finito de termos não nulos.

Exemplos

1º) $f = (4, 3, 2, 1, 0, 0, 0, \ldots, 0, \ldots)$, onde $a_i = 0$ para $i > 3$, é um polinômio sobre o anel $\mathbb{Z}$.

2º) $(0, 0, 0, \ldots, 0, \ldots)$, onde 0 indica o zero do anel A, é um polinômio sobre A, denominado *polinômio nulo*. Aqui o índice r, que figura na definição acima, é o número natural 0, por exemplo.

3º) Se A é um anel com unidade e 1 indica a unidade de A, então as seqüências $(1, 0, 0, 0, \ldots, 0, \ldots)$ e $(0, 1, 0, 0, \ldots, 0, \ldots)$ são polinômios sobre A. Já a seqüência $(1, 1, 1, \ldots, 1, \ldots)$ não é um polinômio sobre A.

4^{o}) Dado o anel $\mathbb{Z}\times\mathbb{Z}$ (produto direto), a seqüência ((1, 1), (1, 1), (0, 0), (0, 0), . . . , (0, 0), . . .) é um polinômio sobre A, enquanto que ((1, 0, (1, 0), (1, 0) , . . . , (1, 0), . . .) não é.

Notação: Indicaremos por A[X] o conjunto dos polinômios sobre o anel A.

Proposição 1: A soma de dois polinômios sobre A é também um polinômio sobre A, isto é, A[X] é fechado em relação à operação de adição.

Demonstração: Sejam $f = (a_i)$ e $g = (b_i)$ dois polinômios sobre A.

Por definição, existe $r_0 \in \mathbb{N}$ tal que $a_i = 0$ para todo $i > r_0$ e também existe $r_1 \in \mathbb{N}$ tal que $b_i = 0$ para todo $i > r_1$. Seja $r = \text{máx}\{r_0, r_1\}$. Temos, então, $a_i + b_i = 0 + 0 = 0$ para todo $i > r$. Assim, $f + g = (a_i + b_i)$ é um polinômio sobre A. ■

Observação: Acabamos de provar que a adição de seqüências sobre A, quando restrita a A[X], também é uma lei de composição interna.

Proposição 2: O produto de dois polinômios sobre A é também um polinômio sobre A, isto é, A[X] é fechado em relação à operação de multiplicação.

Demonstração: Sejam $f = (a_i)$ e $g = (b_j)$ dois polinômios sobre A.

Por hipótese, existe $r_0 \in \mathbb{N}$ tal que $a_i = 0$ para todo $i \geqslant r_0$ e também existe $r_1 \in \mathbb{N}$ tal que $b_j = 0$ para todo $j \geqslant r_1$. Então o termo $c_{r_0 + r_1 + k}$, $\forall k \geqslant 1$, é tal que:

$$c_{r_0 + r_1 + k} = \sum a_i b_{r_0 + r_1 + k - i} =$$

$$= a_0 b_{r_0 + r_1 + k} + a_1 b_{r_0 + r_1 + k - 1} + \ldots + a_{r_0} b_{r_1 + k} + a_{r_0 + 1} b_{r_1 + k - 1} + \ldots +$$

$$+ a_{r_0 + r_1 + k} b_0$$

Como $b_{r_0 + r_1 + k} = b_{r_0 + r_1 + k - 1} = \ldots = b_{r_1 + k} = 0$ e

$a_{r_0 + r_1 + k} = a_{r_0 + r_1 + k - 1} = \ldots = a_{r_0 + 1} = 0$, decorre $c_{r_0 + r_1 + k} = 0$. ■

Observação: Acabamos de provar que a multiplicação de seqüências sobre A, quando restrita a A[X], também é uma lei de composição interna.

Dispositivo prático

Para multiplicar o polinômio $f = (a_0, a_1, a_2, \ldots, a_n, 0, \ldots)$ por $g = (b_0, b_1, b_2, \ldots, b_m, 0, \ldots)$ podemos usar um dispositivo prático assim construído: colocamos numa tabela os coeficientes a_i de f e os b_i de g; calculamos todos os produtos $a_i b_j$; somamos os produtos em cada diagonal, conforme indica a figura, obtendo c_k .

f \ g	b_0	b_1	b_2	b_3	b_4	b_5
a_0	a_0b_0	a_0b_1	a_0b_2	a_0b_3	a_0b_4	a_0b_5
a_1	a_1b_0	a_1b_1	a_1b_2	a_1b_3	a_1b_4	a_1b_5
a_2	a_2b_0	a_2b_1	a_2b_2	a_2b_3	a_2b_4	a_2b_5
a_3	a_3b_0	a_3b_1	a_3b_2	a_3b_3	a_3b_4	a_3b_5
a_4	a_4b_0	a_4b_1	a_4b_2	a_4b_3	a_4b_4	a_4b_5
a_5	a_5b_0	a_5b_1	a_5b_2	a_5b_3	a_5b_4	a_5b_5

Por exemplo, se $f = (4, 3, 2, 1, 0, \ldots, 0, \ldots)$ e $g = (5, 6, 0, \ldots, 0, \ldots)$, temos

f \ g	5	6	0
4	20	24	0
3	15	18	0
2	10	12	0
1	5	6	0
0	0	0	0

$c_0 = 20$
$c_1 = 15 + 24 = 39$
$c_2 = 10 + 18 = 28$
$c_3 = 5 + 12 = 17$
$c_4 = 6$

portanto, $h = f \cdot g = (20, 39, 28, 17, 6, 0, 0, \ldots, 0, \ldots)$.

Proposição 3: Se A é um anel, então A[X] também é um anel.

Demonstração

(i) $f + (g + h) = (f + g) + h$, $\forall$ f, g, h $\in$ A[X]

Fazendo $f = (a_i)$, $g = (b_i)$, $h = (c_i)$, $f + (g + h) = (d_i)$ e $(f + g) + h = (e_i)$, temos:

$d_i = a_i + (b_i + c_i) = (a_i + b_i) + c_i = e_i$, $\forall$ $i \in \mathbb{N}$

(ii) $f + g = g + f$, $\forall$ f, g $\in$ A[X]

Fazendo $f = (a_i)$, $g = (b_i)$, $f + g = (c_i)$ e $g + f = (d_i)$, temos:

$c_i = a_i + b_i = b_i + a_i = d_i$, $\forall$ $i \in \mathbb{N}$.

(iii) $\exists\ e_a \in A[X] \mid f + e_a = f,\ \forall\ f \in A[X]$

Fazendo $f = (a_i)$ e $e_a = (x_i)$, temos:

$f + e_a = f \iff a_i + x_i = a_i,\ \forall\ i \in \mathbb{N}$

então $x_i = 0,\ \forall\ i \in \mathbb{N}$, portanto:

$e_a = (0, 0, 0, \ldots, 0, \ldots) = 0'$

é o elemento neutro para a adição de polinômios, chamado *polinômio nulo.*

(iv) $\forall\ f \in A[X],\ \exists\ f' \in A[X] \mid f + f' = e_a$

Fazendo $f = (a_i)$ e $f' = (x_i)$, temos:

$f + f' = e_a \iff a_i + x_i = 0,\ \forall\ i \in \mathbb{N}$

então $x_i = -a_i,\ \forall\ i \in \mathbb{N}$, portanto:

$f' = (-a_0, -a_1, -a_2, \ldots, -a_i, \ldots) = -f$

é o simétrico aditivo de f, i.e., é o polinômio que somado com f dá o polinômio nulo.

(v) $f \cdot (g \cdot h) = (f \cdot g) \cdot h,\ \forall\ f, g, h \in A[X]$

Fazendo $f = (a_i)$, $g = (b_j)$, $h = (c_k)$, $gh = (d_\ell)$, $f(gh) = (e_m)$, $fg = (x_n)$ e $(fg)h = (y_m)$ temos:

$$e_m = \sum_{i+\ell=m} a_i d_\ell = \sum_{i+\ell=m} a_i \Big(\sum_{j+k=\ell} b_j c_k \Big) = \sum_{i+j+k=m} a_i (b_j c_k) = \sum_{i+j+k=m} (a_i b_j) c_k =$$

$$= \sum_{n+k=m} \Big(\sum_{i+j=n} a_i b_j \Big) c_k = \sum_{n+k=m} x_n c_k = y_m\ ,\ \forall\ m \in \mathbb{N}.$$

(vi) $f \cdot (g + h) = f \cdot g + f \cdot h$ e $(g + h) \cdot f = g \cdot f + h \cdot f, \forall\ f, g, h \in A[X]$

Fazendo $f = (a_i)$, $g = (b_j)$, $h = (c_j)$, $f \cdot (g + h) = (d_k)$, $f \cdot g = (e_k)$ e $f \cdot h = (e'_k)$, temos:

$$d_k = \sum_{j+i=k} a_i (b_j + c_j) = \sum_{i+j=k} a_i b_j + \sum_{i+j=k} a_i c_j = e_k + e'_k$$

para todo $k \in \mathbb{N}$, portanto, $f(g + h) = fg + fh$.

Analogamente se prova a distributividade à direita. ■

Proposição 4: Se A é um anel comutativo, então A[X] também é.

Demonstração: Provemos que $f \cdot g = g \cdot f,\ \forall\ f \cdot g \in A[X]$.

Fazendo $f = (a_i)$, $g = (b_j)$, $fg = (c_k)$ e $gf = (d_k)$, temos:

$$c_k = \sum_{i+j=k} a_i b_j = \sum_{i+j=k} b_j a_i = d_k\ ,\ \forall\ k \in \mathbb{N}.$$ ■

Proposição 5: Se A é um anel com unidade, então A[X] também é.

Demonstração:

Sejam $f = (a_0, a_1, a_2, \ldots, a_i, \ldots)$ e $e_m = (1, 0, 0, \ldots, 0, \ldots)$ em A[X]. É imediato verificar que:

$$e_m \cdot f = f = f \cdot e_m$$

portanto, a unidade de A[X] é e_m. ■

Proposição 6: Se A é um anel de integridade, então A[X] também é.

Demonstração

Sejam $f = (a_0, a_1, \ldots, a_m, 0, \ldots)$ e $g = (b_0, b_1, \ldots, b_n, 0, \ldots)$ dois polinômios não nulos de A[X] tais que $a_m \neq 0$ e $a_{m+i} = 0,\ \forall i \in \mathbb{N}$, $b_n \neq 0$ e $b_{n+i} = 0,\ \forall i \in \mathbb{N}$.

Se $fg = (c_k)$, calculemos c_{m+n} :

$c_{m+n} = a_0 b_{m+n} + a_1 b_{m+n-1} + \ldots + a_m b_n + \ldots + a_{m+n} b_0 = a_m\ b_n \neq 0$ pois a_m e b_n são elementos não nulos do anel de integridade A. Logo $fg \neq 0$. ■

3. GRAU DE UM POLINÔMIO

Definição: Seja $f = (a_i)$ um polinômio não nulo. Chama-se *grau de f,* e representa-se por ∂f ou grf, o número natural n tal que $a_n \neq 0$ e $a_i = 0$ para todo $i > n$. O termo a_n nessas condições é chamado *coeficiente dominante* de f. Se o coeficiente dominante de f é 1, diz-se que f é um *polinômio unitário.*

Exemplos

1º) $f = (4, 7, 0, \underset{a_3}{2}, 0, 0, 0, \ldots)$ em $\mathbb{Z}[X]$ tem grau 3

2º) $g = (-1, \underset{a_4}{\frac{1}{2}}, 0, 5, -1, 0, 0, \ldots)$ em $\mathbb{Q}[X]$ tem grau 4

3º) $h = \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \ldots \right)$ em $(M_2(\mathbb{Z}))[X]$

tem grau 0.

Proposição 7: Se $f = (a_i)$ e $g = (b_i)$ são dois polinômios não nulos de $A[X]$, então:

a) ou $f + g = 0$ ou $\partial(f + g) \leqslant \max\{\partial f, \partial g\}$;

b) $\partial(f + g) = \max\{\partial f, \partial g\}$ quando $\partial f \neq \partial g$

Demonstração

a) Sendo $f + g = (c_i)$ e $n = \max\{\partial f, \partial g\}$, temos:

$c_i = a_i + b_i = 0 + 0 = 0, \ \forall \ i > n$

portanto, ou $f + g = 0$ ou $\partial(f + g) \leqslant n$.

b) Admitindo, por exemplo, $n = \partial f > \partial g$ temos:

$c_n = a_n + b_n = a_n + 0 = a_n \neq 0$ e $c_i = 0, \ \forall \ i > n$

ficando provado que $\partial(f + g) = n$. ■

Exemplos

1º) Em $\mathbb{R}[X]$, se $f = (4, 5, -1, 7, 2, 0, 0, \ldots, 0, \ldots)$ e $g = (1, 7, 4, 0, 0, 0, \ldots, 0, \ldots)$, então $f + g = (5, 12, 3, 7, 2, 0, \ldots, 0, \ldots)$
Neste caso, $\partial(f + g) = 4 = \max\{\partial f = 4, \partial g = 2\}$.

2º) Em $\mathbb{Z}[X]$, se $f = (7, 3, -2, 0, 0, \ldots, 0, \ldots)$ e $g = (-7, -3, 2, 0, 0, \ldots, 0, \ldots)$, então $f + g = (0, 0, 0, \ldots, 0, \ldots)$.

Neste caso, não existe $\partial(f + g)$.

3º) Em $\mathbb{Z}_4[X]$, se $f = (\overline{1}, \overline{2}, \overline{3}, \overline{0}, \ldots, \overline{0}, \ldots)$ e $g = (\overline{2}, \overline{1}, \overline{1}, \overline{0}, \ldots, \overline{0}, \ldots)$, então $f + g = (\overline{3}, \overline{3}, \overline{0}, \overline{0}, \ldots, \overline{0}, \ldots)$.
Neste caso, $\partial(f + g) = 1 < \max\{\partial f = 2, \partial g = 2\}$

Proposição 8: Se $f = (a_i)$ e $g = (b_j)$ são dois polinômios não nulos de $A[X]$, então:

a) ou $f \cdot g = 0$ ou $\partial(f \cdot g) \leqslant \partial f + \partial g$;

b) $\partial(f \cdot g) = \partial f + \partial g$ quando o coeficiente dominante de f ou g é regular em A.

Demonstração

a) Sendo $\partial f = m$, $\partial g = n$ e $f \cdot g = (c_k)$, temos:

$$c_{m+n+p} = a_0 b_{m+n+p} + a_1 b_{m+n+p-1} + \ldots + a_m b_{n+p} + \ldots + a_{m+n+p} b_0$$

e, como $b_j = 0$ para $j > n$ e $a_i = 0$, para $i > m$, decorre $c_{m+n+p} = 0$, $\forall p \in \mathbb{N}$. Assim, ou $f \cdot g = 0$ ou $\partial(f \cdot g) \leqslant m + n$.

b) Se $\partial f = m$ e $\partial g = n$, temos:

$$c_{m+n} = a_0 b_{m+n} + a_1 b_{m+n-1} + \ldots + a_m b_n + \ldots + a_{m+n} b_0 = a_m b_n$$

e, como a_m ou b_n é elemento regular de A, decorre $a_m b_n \neq 0$, isto é, $c_{m+n} \neq 0$ e, portanto, $\partial(f \cdot g) = m + n$. ■

Exemplos

1º) Em $\mathbb{R}[X]$, se $f = (4, 3, 0, 0, 0, \ldots, 0, \ldots)$ e $g = (1, 2, 5, 0, 0, \ldots, 0, \ldots)$, então $f \cdot g = (4, 11, 26, 15, 0, 0, \ldots, 0, \ldots)$
Neste caso, $\partial(f \cdot g) = 3 = \underset{\displaystyle 1}{\underset{\|}{\partial f}} + \underset{\displaystyle 2}{\underset{\|}{\partial g}}$.

2º) Em $\mathbb{Z}_4[X]$, $f = (\overline{2}, \overline{2}, \overline{0}, \overline{0}, \ldots, \overline{0}, \ldots)$ tem grau 1 e $g = (\overline{0}, \overline{0}, \overline{2}, \overline{0}, \ldots, \overline{0}, \ldots)$ tem grau 2, porém, $f \cdot g = (0, 0, 0, \ldots, 0, \ldots)$ não tem grau.

3º) Em $\mathbb{Z}_6[X]$, $f = (\overline{2}, \overline{1}, \overline{3}, \overline{0}, \overline{0}, \ldots, \overline{0}, \ldots)$ tem grau 2 e $g = (\overline{1}, \overline{2}, \overline{0}, \overline{0}, \ldots, \overline{0}, \ldots)$ tem grau 1, porém, $f \cdot g = (\overline{2}, \overline{5}, \overline{5}, \overline{0}, \ldots \overline{0}, \ldots)$ tem grau 2, isto é, $\partial(f \cdot g) < \partial f + \partial g$.

4. IMERSÃO DE A EM A[X]

É evidente, pela construção feita, que A e A[X] são conjuntos cujos elementos são de natureza distinta. É possível, porém, em termos de isomorfismo, supor $A \subset A[X]$. Vejamos como se faz isto.

Proposição 9: Se A é um anel, então $L = \{(a, 0, 0, \ldots, 0, \ldots) \mid a \in A\}$ é um subanel de A[X].

Demonstração

i) $L \neq \phi$ pois $(0, 0, 0, \ldots, 0, \ldots) \in L$.

ii) Se $f = (a, 0, 0, \ldots, 0, \ldots) \in L$ e $g = (b, 0, 0, \ldots, 0, \ldots)$, então $f - g = (a - b, 0, 0, \ldots, 0, \ldots) \in L$ e $fg = (ab, 0, 0, \ldots, 0, \ldots) \in L$. ■

Proposição 10: Sendo A um anel, A é isomorfo ao subanel $L = \{(a, 0, 0, \ldots, 0, \ldots) \mid a \in A\}$ de A[X].

Demonstração: Consideremos agora a aplicação $F: A \longrightarrow L$ dada por $F(x) = (x, 0, 0, \ldots, 0, \ldots)$. Provemos que F é um isomorfismo:

i) $F(a + b) = (a + b, 0, 0, \ldots, 0, \ldots) = (a, 0, 0, \ldots) + (b, 0, 0, \ldots) =$
$= F(a) + F(b), \quad \forall\ a, b \in A.$

ii) $F(ab) = (ab, 0, 0, \ldots, 0, \ldots) = (a, 0, 0, \ldots) \cdot (b, 0, 0, \ldots) = F(a) \cdot F(b)$, $\forall\ a, b \in A.$

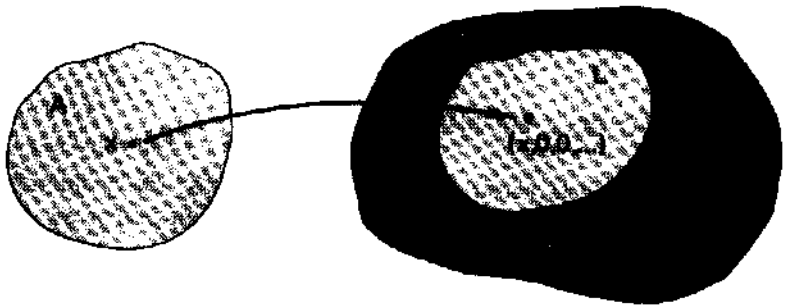
iii) Dados $a, b \in A$ tais que $F(a) = F(b)$, temos:
$F(a) = F(b) \Longrightarrow (a, 0, 0, \ldots) = (b, 0, 0, \ldots) \Longrightarrow a = b$
portanto F é injetora.

iv) Dados $(x, 0, 0, \ldots) \in L$, é imediato que $(x, 0, 0, \ldots) = F(x)$, portanto F é sobrejetora. ■

Devido ao isomorfismo de A e L, podemos identificar cada $a \in A$ ao polinômio $(a, 0, 0, \ldots) \in L$.

$$\boxed{a = (a, 0, 0, \ldots, 0, \ldots)}$$

Aceita esta igualdade, temos em particular que $0 = (0, 0, 0, \ldots, 0, \ldots)$ e $1 = (1, 0, 0, \ldots, 0, \ldots)$ e, ainda, $A = L$ e, portanto, $\boxed{A \subset A[X]}$



Os elementos de A, que agora são polinômios especiais, passam a ser chamados *polinômios constantes*. Convém observar que se $a \in A$ e $g = (b_0, b_1, b_2, \ldots, b_n, 0, \ldots, 0, \ldots) \in A[X]$, então:

$$ag = (a, 0, 0, \ldots)(b_0, b_1, b_2, \ldots, b_n, 0, 0, \ldots) =$$
$$= (ab_0, ab_1, ab_2, \ldots, ab_n, 0, 0, \ldots).$$

5. NOTAÇÃO USUAL DOS POLINÔMIOS

Seja A um anel com unidade. Mostraremos que neste caso é possível, mediante certas convenções, representar um polinômio, segundo a nossa definição, de maneira parecida com aquela com que os polinômios se apresentam em Álgebra Elementar. Há vantagens de ordem prática nisso.

Consideremos o polinômio

$$\boxed{X = (0, 1, 0, 0, \ldots, 0, \ldots)}$$

que é denominado *indeterminada* sobre A. Lembrando a definição de produto de polinômios, temos:

$$X^2 = X \cdot X = (0, 0, 1, 0, 0, \ldots, 0, \ldots)$$
$$X^3 = X^2 \cdot X = (0, 0, 0, 1, 0, \ldots, 0, \ldots)$$

e, assim por diante, X^n é um polinômio em que os n primeiros termos são nulos, $a_n = 1$ e os termos que seguem a_n são todos nulos.

Dado um polinômio $f = (a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots)$ em A[X], temos:

$$f = (a_0, 0, 0, \ldots, 0, 0, 0, \ldots) + (0, a_1, 0, \ldots, 0, 0, 0, \ldots) +$$
$$+ (0, 0, a_2, \ldots, 0, 0, 0, \ldots) + \ldots + (0, 0, 0, \ldots, a_n, 0, 0, \ldots) =$$
$$= a_0 + a_1(0, 1, 0, \ldots, 0, 0, 0, \ldots) + a_2(0, 0, 1, \ldots, 0, 0, 0, \ldots) + \ldots +$$
$$+ a_n(0, 0, 0, \ldots, 1, 0, 0, \ldots) = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$$

A notação $f = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$ é a *notação polinomial* ou *notação usual* para indicar um polinômio f sobre um anel com unidade. Isso explica inclusive, para os casos de anéis com unidade, o porquê da notação A[X]. Para os demais anéis de polinômios que, aliás, não mais serão focalizados daqui para a frente, a notação A[X] foi usada apenas para manter a uniformidade.

Nota: Do que vimos nos últimos dois itens, podemos concluir que todo elemento $a \in A$ é um particular polinômio (polinômio constante) e:

$a = (a, 0, 0, \ldots, 0, \ldots)$ ou
$a = a + 0X + 0X^2 + \ldots$ (se A possuir unidade).

6. POLINÔMIOS INVERSÍVEIS

Como A é um subanel unitário de A[X] é claro que $U(A) \subset U(A[X])$.

Mostremos que se A é um anel de integridade vale a inclusão contrária, isto é, $U(A[X]) \subset U(A)$.

Dado $f \in U(A[X])$, existe $g \in A[X]$ tal que $fg = 1$ e, então, $\partial(fg) = \partial(1)$, isto é, $\partial f + \partial g = 0$. Assim sendo, $\partial f = \partial g = 0$, portanto, $f \in A$ e $g \in A$. Como $fg = 1$, decorre que $f \in U(A)$.

Ficou assim provado que se A é um anel de integridade, então $U(A[X]) = U(A)$.

Exemplos

1º) $U(\mathbb{Z}[X]) = U(\mathbb{Z}) = \{1, -1\}$

2º) $U(\mathbb{R}[X]) = U(\mathbb{R}) = \mathbb{R}^*$

3º) $U(\mathbb{Z}_5[X]) = U(\mathbb{Z}_5) = \mathbb{Z}_5^*$

Quando A *não* é anel de integridade pode ocorrer que $U(A) \subsetneq U(A[X])$, isto é, podem existir polinômios não constantes mas inversíveis. Por exemplo em $\mathbb{Z}_4[X]$ o polinômio $f = \overline{1} + \overline{2}X$ é inversível pois

$$ff = (\overline{1} + \overline{2}X)(\overline{1} + \overline{2}X) = \overline{1} + \overline{4}X + \overline{4}X^2 = \overline{1}.$$

7. DERIVADA FORMAL DE UM POLINÔMIO

Conceito: Chama-se *derivada formal* de um polinômio

$$f = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n \in A[X]$$

onde A é um anel com unidade, o seguinte polinômio de A[X]:

$$f' = a_1 + 2a_2X + \ldots + na_nX^{n-1}.$$

Por recorrência pode-se definir a derivada de ordem r do polinômio f, denotada por $f^{(r)}$, da seguinte maneira:

1) $f^{(0)} = f$

2) $f^{(r)} = (f^{(r-1)})'$, $\forall \quad r > 0$.

Teremos assim sucessivamente: $f^{(0)} = f$, $f^{(1)} = f'$, $f^{(2)} = (f')'$, ...

Valem as seguintes propriedades:

(i) $(f + g)' = f' + g'$, $\forall \quad f, g \in A[X]$;

(ii) Se $f \in A$, então $f' = 0$;

(iii) $(fg)' = f'g + fg'$, $\forall \quad f, g \in A[X]$.

Justificaremos apenas a última dessas propriedades. As duas primeiras são muito fáceis de verificar e as deixamos como exercícios.

1º caso: f = c (constante) e g qualquer

Supondo $g = b_0 + b_1X + \ldots + b_nX^n$, então $cg = (cb_0) + (cb_1)X + \ldots + (cb_n)X^n$ e $(cg)' = (cb_1) + 2(cb_2)X + \ldots + n(cb_n)X^{n-1}$.

Por outro lado, $c'g + cg' = 0 \cdot g + c(b_1 + 2b_2X + \ldots + nb_nX^{n-1})$.

Donde $(cg)' = c'g + cg' = cg'$.

Obtivemos assim, inclusive uma regra para a derivada formal do produto de um polinômio constante por um polinômio qualquer.

2º caso: $f = X^h$ e $g = X^k$

Aqui $f' = hX^{h-1}$ e $g' = kX^{k-1}$. Logo $f'g + fg' = hX^{k+h-1} + kX^{k+h-1} = (h + k)X^{h+k-1}$.

Como $fg = X^{h+k}$, então $(fg)' = (h + k)X^{h+k-1}$.

Caso geral

Sejam $f = \sum_{h=0}^{m} a_hX^h$ e $g = \sum_{k=0}^{n} b_kX^k$. Então $fg = \sum_h \sum_k a_hb_kX^hX^k$

Levando em conta (i) e a observação ao fim do 1º caso achamos

$$(fg)' = \sum_h \sum_k a_hb_k(X^hX^k)'$$

Observando o que se concluiu no 2º caso chega-se então a

$$(fg)' = \sum_h \sum_k a_hb_k[(X^h)'X^k + X^h(X^k)'].$$

Daí:

$$(fg)' = \sum_h a_h(X^h)' \sum_k b_kX^k + \sum_h a_hX^h \sum_k b_k(X^k)'$$

ou seja,

$$(fg)' = f'g + fg' \qquad \blacksquare$$

EXERCÍCIOS

1. Determinar todos os polinômios de grau 1 do anel $\mathbb{Z}_3[X]$. Quantos são os polinômios de grau p do anel $\mathbb{Z}_n[X]$? Quantos são os polinômios unitários e de grau p do anel A[X] onde A é um anel comutativo e com unidade, com n elementos ?

2. Escrever sob a forma usual os seguintes polinômios de A[X].

a) $(2 + 3X + X^2) + (2 + 2X + 3X^2)$, $A = \mathbb{Z}_4$

b) $(2 + 3X + 2X^2) \cdot (1 + 2X^2)$, $A = \mathbb{Z}_4$

c) $X(X - 1)(X - 2)$, $A = \mathbb{Z}_3$

d) $(1 + X + X^2)^2$, $A = \mathbb{Z}_2$

e) $(1 + 2X^2)^9$, $A = \mathbb{Z}_3$

3. Se $f = (1, 2) + (2, 0)X$, $g = (1, -1)X + (1, 1)X^2$ e $h = (-4, -1) + (-2, 1)X$, calcular $f + g + h$, $fg - h^2$ e $fh + g$. Todos os polinômios estão em $(\mathbb{Z} \times \mathbb{Z})[X]$.

4. Se $f = a + bX$, $g = c + bX + aX^2$ e $h = b + cX^2$ são polinômios do anel $(M_2(\mathbb{Z}))[X]$ onde $a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ $b = \begin{pmatrix} 0 & 2 \\ 3 & 0 \end{pmatrix}$ e $c = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}$, calcular f^2, $f^2 - g^2$, $g^2 + 2gh + h^2$ e h^3.

5. Seja A um anel de integridade. Se $f, g \in A[X]$, $f \neq 0$ e $g \neq 0$, mostre que $\partial(f \cdot g) = \partial(f) + \partial(g)$.

6. Determinar os graus dos seguintes polinômios de $A[X]$:

   a) $(1 + X^2)^3 (1 - X^2)^2$, $A = \mathbb{Q}$

   b) $(1 + X^2)^3 (1 - X^2)^3 + X^2$, $A = \mathbb{Z}_3$

   c) $(1 + X + X^2 + X^3 + X^4)^7$, $A = \mathbb{Z}_7$

   d) $(1 + 2X^2)^4$, $A = \mathbb{Z}_8$.

7. Mostre que não existe $f \in \mathbb{R}[X]$ tal que $f^2 = 1 + X + X^3$.

8. Obter a e b em $\mathbb{Z}_5$ para que $X^4 + 3X^3 + 2X^2 + aX + b$ seja um quadrado perfeito em $\mathbb{Z}_5[X]$.

9. Ache $a \in K$ de modo que aX^2 seja um quadrado perfeito em $K[X]$ nos seguintes casos:

   a) $K = \mathbb{Q}$ b) $K = \mathbb{R}$ c) $K = \mathbb{C}$

10. Se f e g são polinômios do anel $A[X]$ tais que $\partial f^2 = 8$ e $\partial(fg) = 7$, determine $\partial(f + g)$, $\partial(f - g)$, ∂f^3, ∂g^2 e $\partial(f^3 + 3f^2g + 3fg^2 + g^3)$, sabendo que A é um anel de integridade.

11. Sejam $f, g \in A[X]$ (A = anel de integridade) tais que $\partial(f + g) = 5$ e $\partial(f - g) = 2$. Ache os graus de $f \cdot g$, $f^2 - g^2$ e $f^2 + g^2$.

12. Encontre um polinômio não constante inversível no anel $\mathbb{Z}_8[X]$.

13. Mostre que $1 + 2X^2 + 2X^3 \in \mathbb{Z}_4[X]$ é inversível.

14. Sabendo que o polinômio $f = (c - a - 1) + (b - c + 5)X + (a - b - 2)X^2 + (a - 1)X^3$ tem inverso multiplicativo no anel $\mathbb{R}[X]$, obter a, b, c e f^{-1}.

15. Seja A um anel tal que $\exists\ a \in A$ de modo que $a^2 = 0$. Mostre que $f = 1 + aX \in A[X]$ é inversível.

16. Mostre que o polinômio X não é inversível. Que conclusão isto acarreta no que tange à estrutura de $A[X]$?

§ 2º — DIVISÃO EM A [X]

Deste parágrafo em diante somente consideraremos polinômios sobre um anel comutativo com unidade ou situações mais particulares que serão fixadas na ocasião oportuna.

1. DIVISÃO

Dado um anel A (conforme observação acima), se $f, g \in A[X]$, diz-se que f *divide* g ou que g é *divisível* por f se existe $h \in A[X]$ tal que $g = fh$.

Notação: $f \mid g$. Se f não divide g escreve-se $f \nmid g$.

Exemplo: Sejam $f = 1 + X$ e $g = 1 - X^2$ em $\mathbb{Z}[X]$. Como $1 - X^2 = (1 + X)(1 - X)$ e $1 - X \in \mathbb{Z}[X]$, pode-se dizer que $f \mid g$.

A relação dada por "f divide g", sobre o anel $A[X]$, tem as seguintes propriedades:

(i) $f \mid f$, $\forall\ f \in A[X]$;

(ii) $f \mid g$ e $g \mid h \implies f \mid h$;

(iii) $f \mid g \implies f \mid hg$, $\forall\ h \in A[X]$;

(iv) $f \mid g_1$ e $f \mid g_2 \implies f \mid (g_1 h_1 + g_2 h_2)$, $\forall\ h_1, h_2 \in A[X]$.

Provemos (iv).

$$\left.\begin{array}{l} f \mid g_1 \implies \exists\ q_1 \in A[X] \text{ tal que } g_1 = fq_1 \\ f \mid g_2 \implies \exists\ q_2 \in A[X] \text{ tal que } g_2 = fq_2 \end{array}\right\} \implies g_1 h_1 + g_2 h_2 = f(h_1 q_1 + h_2 q_2) \implies$$

$$\implies f \mid (g_1 h_1 + g_2 h_2). \quad \blacksquare$$

2. ALGORÍTMO DA DIVISÃO (ou de Euclides)

Observemos os polinômios $f = 1 + X^2 \in \mathbb{Z}[X]$ e $g = 1 - X \in \mathbb{Z}[X]$. É claro que $f \nmid g$. Por outro lado g também não divide f pois

$1 + X^2 = (1 - X)(a + bX) \implies 1 + X^2 = a + (b - a)X - bX^2 \implies a = 1, b - a = 0$ e $-b = 1 \implies b = 1$ e $b = -1$ (absurdo).

Veremos agora que, sob certas condições, quando ocorre o que se viu no exemplo acima, é possível conseguir uma "divisão aproximada" nos moldes daquela já conhecida no anel $\mathbb{Z}$.

Teorema 1: Dados $f = a_0 + a_1X + \ldots + a_nX^n$ e $g = b_0 + b_1X + \ldots + b_mX^m$ em A[X], suponhamos $g \neq 0$ e o coeficiente dominante de g inversível. Nessas condições existem $q, r \in A[X]$ de modo que $f = gq + r$, onde $r = 0$ ou $\partial(r) < \partial(g)$.

Demonstração

(a) $f = 0$. Neste caso $q = r = 0$, pois $0 = g \cdot 0 + 0$.

(b) $f \neq 0$ e $\partial(f) < \partial(g)$. Quando isto acontece basta tomar $q = 0$ e $r = f$, porque $g \cdot 0 + f = f$ e, por hipótese, $\partial(f) < \partial(g)$.

(c) $\partial(f) \geqslant \partial(g)$. Procede-se por indução (segundo princípio).

Se $\partial(f) = 0$, então $\partial(g) = 0$. Daí $f = a_0$ e $g = b_0$ (coeficiente dominante de g neste caso). Basta pois tomar $q = b_0^{-1}a_0$ e $r = 0$ uma vez que $a_0 = b_0(b_0^{-1}a_0) + 0$.

Suponhamos agora que $\partial(f) = n$ e que o teorema se verifique para todo polinômio de grau menor que n.

Consideremos o polinômio

$$f_1 = f - a_nb_m^{-1}X^{n-m}g$$

Se $f_1 = 0$ ou $\partial(f_1) < \partial(g)$, então $r = f_1$ e $q = a_nb_m^{-1}X^{n-m}$. Caso contrário tem-se $\partial(f_1) \leqslant n-1$ e $\partial(f_1) \geqslant \partial(g)$. Pela hipótese de indução existem $q_1, r_1 \in A[X]$ de maneira que

$$f_1 = gq_1 + r_1, \text{ onde } r_1 = 0 \text{ ou } \partial(r_1) < \partial(g).$$

Então

$$f - a_nb_m^{-1}X^{n-m}g = gq_1 + r_1$$

o que acarreta que

$$f = g(q_1 + a_nb_m^{-1}X^{n-m}) + r_1, \text{ onde } r_1 = 0 \text{ ou } \partial(r_1) < \partial(g).$$

Isso prova o teorema. ■

Corolário 1: Se A é um anel de integridade, então é único o par (q, r) de polinômios que figuram no enunciado do teorema.

Demonstração: Vamos supor $f = gq + r = gq_1 + r_1$, onde $\partial(r) < \partial(g)$ se $r \neq 0$ e $\partial(r_1) < \partial(g)$, se $r_1 \neq 0$. Então $g(q - q_1) = r_1 - r$. Como A[X] é um anel de integridade, então $r_1 - r = 0$ se, e somente se, $q - q_1 = 0$.

Suponhamos $r_1 \neq r$. Então se pode calcular

$$\partial(g(q - q_1)) = \partial(g) + \partial(q - q_1) = \partial(r_1 - r).$$

Logo $\partial(r_1 - r) \geqslant \partial(g)$ o que é impossível pois $\partial(r_1 - r) = \partial(r_1)$ ou $\partial(r_1 - r) = \partial(r)$ ou ou $\partial(r_1 - r) < \max\{\partial(r_1), \partial(r)\}$. ■

Corolário 2: Seja A um corpo. Dados $f, g \in A[X]$ com $g \neq 0$, existe um único par (q, r) de polinômios de A[X] de forma que $f = gq + r$ e $\partial(r) < \partial(g)$ quando $r \neq 0$.

Demonstração: É só levar em conta que todo elemento não nulo de um corpo é inversível e observar o corolário anterior. ■

Nota: Os polinômios q e r cuja existência nos é assegurada pelo teorema 1 acima são chamados, respectivamente, *quociente* e *resto* na divisão euclidiana de f por g.

Exemplo

Determinemos o quociente e o resto na divisão euclidiana de $f = X^3 - 1$ por $g = X + 3$, ambos de $\mathbb{Z}[X]$. Como o coeficiente dominante de g é 1 (inversível), então isso é possível em $\mathbb{Z}[X]$.

Adotemos o seguinte dispositivo

$$\begin{array}{r|l} X^3 + 0X^2 + 0X - 1 & X + 3 \\ \cline{2-2} -X^3 - 3X^2 & X^2 \\ \cline{1-1} -3X^2 + 0X - 1 & \end{array}$$

O polinômio $-3X^2 - 1$ é o primeiro resto parcial, uma vez que seu grau ainda é maior que o de g. Corresponde ao f_1 que apareceu na demonstração do teorema. Aplicar a hipótese de indução a $f_1 = -3X^2 - 1$ com relação a g significa, na prática, seguir com o raciocínio feito. Vejamos.

$$\begin{array}{r|l} X^3 + 0X^2 + 0X - 1 & X + 3 \\ \cline{2-2} -X^3 - 3X^2 & X^2 - 3X + 9 \\ \cline{1-1} -3X^2 + 0X - 1 & \\ 3X^2 + 9X & \\ \cline{1-1} 9X - 1 & \\ -9X - 27 & \\ \cline{1-1} -28 & \end{array}$$

Logo o quociente neste caso é $q = 9 - 3X + X^2$ e o resto é $r = -28$.

EXERCÍCIOS

17. Obter o grau dos polinômios q (quociente) e r (resto) na divisão de f por g em $\mathbb{R}[X]$, nos seguintes casos:

1º) gr f = 5 e gr g = 3

2º) gr f = n e gr g = n − 1, $n \in \mathbb{N}^*$

3º) gr f = n e gr g = m, $m, n \in \mathbb{N}$

18. Determinar o quociente e o resto da divisão euclidiana de f por g, polinômios pertencentes a A[X], nos seguintes casos:

1º) f = 0, $g = 5X^2 - 1$ e $A = \mathbb{Q}$

2º) $f = X^2 - 1$, $g = X^3 + X^2 - 1$ e $A = \mathbb{Z}$

3º) $f = 4X^4 - 6X + 2$, $g = X^2 - 1$ e $A = \mathbb{R}$

4º) $f = 4X^4 - 6X + 2$, $g = 3X^3 - 3X + 2$ e $A = \mathbb{Z}_7$

5º) $f = X^{10} - X$, $g = X^4 + X^3 + 4X^2 + X$ e $A = \mathbb{Z}_{17}$

19. Ache o quociente e o resto da divisão euclidiana de f por g nos seguintes casos:

1º) $f = X + 1$; $g = X^2 + 1$; $A = \mathbb{Z}_2$

2º) $f = (1, 1) + (1, 1)X^2$; $g = (0, 1) + (1, 1)X$ e $A = \mathbb{Z} \times \mathbb{Z}$

3º) $f = (0, 1) + (1, 0)X + (1, 1)X^2$; $g = (0, 1) + (1, 1)X$ e $A = \mathbb{Z}_2 \times \mathbb{Z}_2$

4º) $f = nX^{n+1} - (n+1)X^n + 1$; $g = (X - 1)^2$ e $A = \mathbb{Q}$ $(n \in \mathbb{N}^*)$.

20. Determinar a de modo que a divisão euclidiana de $f = 4X^3 - 6X + a$ por $g = X + 3$ seja exata, supondo que f e g pertençam a $\mathbb{Z}_7[X]$.

21. Determinar a, b, c para que $f = 3X^4 + aX^3 + 6X^2 + bX + c$ seja divisível por $g = X^3 - 5X^2 + 6X$, supondo f e g pertencentes a $\mathbb{Q}[X]$.

22. Determinar a e $b \in \mathbb{Z}$ de modo que o polinômio $f = X^4 + 3X^3 + 2X^2 + aX + b$ dividido por $g = X^2 + X + 1$ dê resto $r = 7X - 5$. Qual é o quociente da divisão?

23. Ache a, $b \in \mathbb{R}$ de modo que o polinômio $f = 1 + 10X + bX^2 + bX^3 + aX^4 + X^5$ seja divisível por $(X - 1)^2$.

24. Sejam f e $g \neq 0$ polinômios do anel K[X], onde K é um corpo. Demonstrar que se q e r são, respectivamente, o quociente e o resto da divisão euclidiana de f por g e se $a \in K^*$, então q e ar são respectivamente o quociente e o resto da divisão euclidiana de af por ag. Aplicando o resultado anterior, calcular q e r na divisão em $\mathbb{Q}[X]$ do polinômio

$$f = X^4 - \frac{1}{2}X^3 + \frac{1}{2}X^2 - \frac{1}{6}X + 2 \quad \text{por} \quad g = X^2 - \frac{1}{6}X + \frac{1}{6}$$

25. Divide-se um polinômio f por X − a, obtendo quociente q_1 e resto r_1. Em seguida, divide-se q_1 por X − b, obtendo quociente q_2 e resto r_2. Expressar o quociente q e o resto r da divisão de f por (X − a)(X − b) em termos de q_1, q_2, r_1, r_2, a e b. Efetuar, usando o resultado anterior, a divisão euclidiana de $f = 5X^4 + 6X^3 + 11X^2 - 1$ por $g = X^2 - 5X + 4$.

26. Seja K um corpo; estude as condições em que a relação sobre K[X] dada por "f | g" é anti-simétrica.

27. Ache os geradores dos seguintes ideais em $\mathbb{Z}[X]$:

$I = \{a_0 + a_1X + \ldots \in \mathbb{Z}[X] \mid a_0 = 0\}$

$J = \{a_0 + a_1X + \ldots \in \mathbb{Z}[X] \mid a_0 \in 2\mathbb{Z}\}$.

28. Dê um exemplo de um anel A comutativo com unidade e de polinômios $f, g \in A[X]$ de modo que o coeficiente dominante de g é inversível e que não sejam únicos quociente e resto na divisão euclidiana de f por g.

29. Representar $1 + X^4$ como um produto de dois polinômios unitários de $\mathbb{R}[X]$, ambos de grau 2. É possível representar $1 + X^4 \in \mathbb{R}[X]$ sob a forma $(X - a) \cdot f$ onde $f \in \mathbb{R}[X]$ e $a \in \mathbb{R}$?

30. Seja K um corpo e considere $a \in K$.

Mostre que se $f = a_0 + a_1X + \ldots + a_nX^n \in K[X]$, então existem $C_0, C_1, \ldots, C_n \in K$ de modo que $f = C_0 + C_1(X - a) + \ldots + C_n(X - a)^n$.

31. Mostre que é um homomorfismo de $\mathbb{Z}[X]$ em $\mathbb{Z}_m[X]$, $\forall\, m > 1$, a aplicação

$F: \mathbb{Z}[X] \longrightarrow \mathbb{Z}_m[X]$ dada por $F(a_0 + a_1X + \ldots + a_rX^r) = \bar{a}_0 + \bar{a}_1X + \ldots + \bar{a}_rX^r$,

$\forall\, a_0 + a_1X + \ldots + a_rX^r \in \mathbb{Z}[X]$.

32. Seja A um anel com unidade. Mostre que $c(A) = c(A[X])$.

33. Mostrar que $\mathbb{Z}[X]$ é um subanel de $\mathbb{Q}[X]$; $\mathbb{Z}[X]$ é um ideal de $\mathbb{Q}[X]$?

34. Verifique se são subanéis de $\mathbb{Z}[X]$ ou ideais em $\mathbb{Z}[X]$:

a) $\{a_0 + a_1X + \ldots \in \mathbb{Z}[X] \mid a_0 \in 2\mathbb{Z}\}$

b) $\{a_0 + a_1X + \ldots \in \mathbb{Z}[X] \mid a_0 = 0\}$

c) $\{a_0 + a_1X + \ldots \in \mathbb{Z}[X] \mid a_0 + a_1 = 0\}$

35. Mostre que o ideal $I = \langle X \rangle$ é primo em $\mathbb{Z}[X]$.

36. Mostre que o ideal $I = \langle 2, X \rangle$ é maximal e não é principal em $\mathbb{Z}[X]$.

Sugestão: Observe o termo de grau zero dos elementos de $\langle 2, X \rangle$ e mostre que se $\langle 2, X \rangle \subset J$ (ideal em $\mathbb{Z}[X]$) então $1 \in J$. Depois verifique que não existe $a \in \mathbb{Z}[X]$, a não inversível, tal que $a \mid 2$ e $a \mid X$.

37. Verifique se $I = \langle 4, X \rangle$ é maximal em $\mathbb{Z}[X]$. É principal? Por que?

§ 3º — RAÍZES DE POLINÔMIOS

1. VALOR DE UM POLINÔMIO

Também neste parágrafo somente consideraremos anéis comutativos com unidade.

Seja B um anel comutativo com unidade e A um subanel unitário de B. Dados $f = a_0 + a_1X + \ldots + a_nX^n \in A[X]$ e $u \in B$, chama-se *valor* de f em u o seguinte elemento de B:

$$f(u) = a_0 + a_1u + \ldots + a_nu^n$$

Quando se verifica a igualdade $f(u) = 0$ (zero de B), dizemos que u é *raiz* de f.

Valem as seguintes propriedades:

(a) $(f + g)(u) = f(u) + g(u)$ e

(b) $(fg)(u) = f(u)g(u)$, $\forall$ f, g $\in A[X]$ e $\forall$ u $\in$ B.

Verifiquemos a segunda delas. Para tanto sejam

$f = a_0 + a_1X + \ldots + a_mX^m$ e $g = b_0 + b_1X + \ldots + b_nX^n$.

Então

$$fg = \sum_{k=0} \Big(\sum_{i+j=k} a_ib_j \Big)X^k \quad \text{e} \quad (fg)(u) = \sum_{k=0}^{m+n} \Big(\sum_{i+j=k} a_ib_j \Big)u^k.$$

Por outro lado, como

$$f(u) = \sum_{i=0}^{m} a_iu^i \quad \text{e} \quad g(u) = \sum_{j=0}^{n} b_ju^j, \text{ então}$$

$$f(u)g(u) = \Big(\sum_{i=0}^{m} a_iu^i \Big)\Big(\sum_{j=0}^{n} b_ju^j \Big) = \sum_{j=0}^{n} \Big(\sum_{i=0}^{m} a_iu^i \Big)b_ju^j = \sum_{j=0}^{n} \sum_{i=0}^{m} a_ib_ju^{i+j} =$$

$$= \sum_{k=0}^{m+n} \Big(\sum_{i+j=k} a_ib_j \Big)u^k. \quad \blacksquare$$

Exemplo: Sejam $A = \mathbb{R}$, $B = \mathbb{C}$, $f = 1 + X^2$, $u = i$ e $v = 1 + i$. Então $f(u) = 1 + i^2 = 1 - 1 = 0$ e $f(v) = 1 + (1 + i)^2 = 1 + 1 + 2i - 1 = 1 + 2i$. Observe-se que i é raiz de f.

2. SOBRE RAÍZES

Proposição 11: Sejam A um anel comutativo com unidade, u um elemento de A e $f = a_0X^n + a_1X^{n-1} + \ldots + a_n \in A[X]$ um polinômio de grau n. Nessas condições: (a) (*teorema do resto*) O resto na divisão euclidiana de f por X - u é f(u); (b) (*algorítmo do Briot-Ruffini*) Se $q = b_0X^{n-1} + b_1X^{n-2} + \ldots + b_{n-1}$ e $r = b_n$ são respectivamente, quociente e resto na divisão considerada, então $b_0 = a_0$, e $b_i = ub_{i-1} + a_i$ $(i = 1, 2, \ldots, n)$.

Demonstração

(a) É óbvio que vale o algorítmo da divisão com respeito a f e X - u pois o coeficiente dominante deste último polinômio é 1. Vamos supor

$f = (X - u)q + r$, onde $r = 0$ ou $\partial(r) = 0$ (pois $\partial(X - u) = 1$).

Achando o valor de f em u:

$f(u) = (u - u)q(u) + r(u) = r$

uma vez que, sendo r constante, $r(u) = r$.

(b) Calculemos $(X - u)q + r$:

$(X - u)(b_0X^{n-1} + b_1X^{n-2} + \ldots + b_{n-2}X + b_{n-1}) + b_n = b_0X^n + (b_1 - ub_0)X^{n-1} + \ldots + \ldots + (b_{n-1} - ub_{n-2})X + (b_n - ub_{n-1})$.

Levando em conta que $(X - u)q + r = f$, obtemos as seguintes igualdades: $b_0 = a_0$, $b_1 - ub_0 = a_1, \ldots, b_{n-1} - ub_{n-2} = a_{n-1}$ e $b_n - ub_{n-1} = a_n$.

Daí:

$b_0 = a_0$, $b_1 = ub_0 + a_1, \ldots, b_{n-1} = ub_{n-2} + a_{n-1}$ e $b_n = ub_{n-1} + a_n$

que são as igualdades pretendidas. $\blacksquare$

Corolário: $f \in A[X]$ é divisível por X - u se, e somente se, $f(u) = 0$.

Demonstração: Decorre diretamente da parte (a) da proposição. $\blacksquare$

Nota: O algorítmo do Briot-Ruffini, dado pela parte (b) da proposição, na prática pode ser efetuado da seguinte maneira:

u	a_0	a_1	$\ldots\ldots\ldots$	a_{n-1}	a_n
		ua_0		ub_{n-2}	ub_{n-1}
	a_0	$ua_0 + a_1 = b_1$	$\ldots$	$ub_{n-2} + a_{n-1} = b_{n-1}$	$ub_{n-1} + a_n = b_n$

Exemplo: No anel $\mathbb{Z}\times\mathbb{Z}$ efetuemos a divisão euclidiana de $f = (1, 1) + (1, 2)X + (1, -1)X^2$ por $X - (-1, 1)$.

$(-1, 1)$	$(1, -1)$	$(1, 2)$	$(1, 1)$
		$(-1, -1)$	$(0, 1)$
	$(1, -1)$	$(0, 1)$	$(1, 2) = r$

Logo $q = (0, 1) + (1, -1)X$ e $r = (1, 2)$.

Proposição 12: Seja A um anel de integridade e $f \in A[X]$ um polinômio não nulo. Então o número de raízes de f em A não ultrapassa $\partial(f)$.

Demonstração: Se o grau de f é zero é imediato o que a proposição afirma pois, neste caso, f não admite nenhuma raiz em A.

Suponhamos agora que $\partial(f) = n > 0$ e que o teorema seja verdadeiro para todo polinômio de grau $n - 1$. Se f não possui nenhuma raiz em A, provado. Caso contrário, se u é uma raiz de f em A, então existe $q \in A[X]$ de modo que $f = (X - u)q$. Daí, qualquer outra raiz de f (caso exista) é raiz de q. De fato:

$v \neq u$ e $f(v) = 0 \Longrightarrow (v - u)q(v) = 0 \Longrightarrow q(v) = 0$ (aqui entrou a hipótese de A é de integridade).

Como o número de raízes de q não ultrapassa $n - 1 = \partial(q)$, então o número de raízes de f em A é, no máximo, n. ■

Corolário: Se f e g são polinômios de grau n sobre um anel de integridade A e se existem $n + 1$ elementos $u_0, u_1, \ldots, u_n \in A$, distintos entre si, tais que $f(u_i) = g(u_i) (i = 0, 1, \ldots, n)$, então $f = g$.

Demonstração: O polinômio $h = f - g$ admite mais do que n raízes em A. Logo $h = 0$, ou seja, $f = g$. ■

Exemplo: O polinômio $f = (1, 0)X^2 \in (\mathbb{Z}\times\mathbb{Z})[X]$ tem grau dois e, no entanto, tem infinitas raízes em $\mathbb{Z}\times\mathbb{Z}$: todo elemento $(0, a) \in \mathbb{Z}\times\mathbb{Z}$ é raiz de f porque

$$f(0, a) = (1, 0)(0, a)^2 = (1, 0)(0, a^2) = (0, 0).$$

Naturalmente isso acontece porque $\mathbb{Z}\times\mathbb{Z}$ não é um anel de integridade.

3. FUNÇÃO POLINOMIAL

Seja A um anel comutativo com unidade. Para cada $f \in A[X]$ é possível definir a função

$$f_A : A \longrightarrow A, \text{ dada por } f_A(u) = f(u), \forall\ u \in A.$$

Logo f_A associa a cada $u \in A$ o valor de f em u. Tal função chama-se *função polinomial* definida por f sobre A. Denotaremos por P(A) o conjunto dessas funções.

Exemplo: Seja $A = \mathbb{Z}_2 = \{0, 1\}$. O polinômio $f = 1 + X + X^3$, por exemplo, nada mais é do que a seqüência $(1, 1, 0, 1, 0, 0, \ldots)$ enquanto que f_A é a função

$$0 \longmapsto f(0) = 1$$
$$1 \longmapsto f(1) = 1$$

Adição em P(A)

A soma de duas funções polinomiais f_A e g_A definida através de

$$(f_A + g_A)(u) = f_A(u) + g_A(u), \ \forall\ u \in A,$$

também é uma função polinomial pois

$(f_A + g_A)(u) = f_A(u) + g_A(u) = f(u) + g(u) = (f + g)(u) = (f + g)_A(u), \forall\ u \in A$, ou seja, $f_A + g_A = (f + g)_A$.

Não oferece nenhuma dificuldade mostrar que, em relação à adição assim definida, P(A) é um grupo abeliano. A associatividade se prova assim:

$f_A + (g_A + h_A) = f_A + (g + h)_A = (f + (g + h))_A = ((f + g) + h)_A = (f + g)_A + h_A = (f_A + g_A) + h_A$.

O elemento neutro é a função definida pelo polinômio nulo e $-f_A$ é a função definida através de $-f$.

Multiplicação em P(A)

Analogamente, o produto de duas funções polinomiais f_A e g_A é a função polinomial $(fg)_A$. Para a multiplicação assim definida valem as propriedades seguintes: (i) associativa (exercício), (ii) Comutativa (exercício), (iii) Existe elemento neutro: é a função definida pelo polinômio constante 1 (unidade de A) e (iv) distributiva em relação à adição (exercício).

Assim, conclui-se que P(A) é um anel comutativo com unidade.

Teorema 2: Se A é um anel de integridade infinito, então A[X] e P(A) são isomorfos através da aplicação $F: A[X] \longrightarrow P(A)$ assim definida:

$$F(f) = f_A, \ \forall\ f \in A[X].$$

Demonstração:

- $F(f+g) = (f+g)_A = f_A + g_A = F(f) + F(g)$, $\forall\ f, g \in A[X]$.
- Analogamente, $F(fg) = F(f)F(g)$, $\forall\ f, g \in A[X]$.
- Dada uma função polinomial h_A é claro que $F(h) = h_A$. Logo F é sobrejetora.
- Sejam $f, g \in A[X]$. Então:

$F(f) = F(g) \Longrightarrow f_A = g_A \Longrightarrow f_A - g_A = 0_A$ (função polinomial nula) $\Longrightarrow$

$\Longrightarrow (f-g)_A = 0_A \Longrightarrow (f-g)_A(u) = 0_A(u),\ \forall\ u \in A \Longrightarrow (f-g)(u) = 0, \forall\ u \in A$

$\Longrightarrow f(u) = g(u),\ \forall\ u \in A.$

Levando em conta o corolário da proposição 12, deste capítulo, e o fato de que A é infinito, concluimos que $f = g$.

Assim ficou provado que F é injetora o que, juntamente com as conclusões anteriores, nos permite afirmar que F é um isomorfismo de anéis. ■

Notas:

a) A proposição acima nos garante que A[X] e P(A) podem ser encarados como o "mesmo" anel, quando A é um anel de integridade infinita. É o que se faz, por exemplo, na Álgebra clássica, quando se define polinômio sobre $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ como sendo toda função dada por

$$x \longmapsto a_0 + a_1x + \ldots + a_nx^n$$

onde os a_i são elementos fixos daquele anel, dentre os quatro citados, que estejamos considerando.

Se A não é um anel de integridade ou se A não é infinito essa identificação não poderá ser feita conforme mostram os exemplos a seguir.

b) O anel $A = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\} = \mathbb{Z}_5$ é um anel de integridade finito. Neste caso a função F definida na proposição anterior não é injetora porque tomando $f = X(X-\overline{1})(X-\overline{2})(X-\overline{3})(X-\overline{4})$ que é, evidentemente, um polinômio não nulo ($\delta(f) = 5$), a função f_A definida por ele é a função polinomial nula, uma vez que, $f(\overline{0}) = f(\overline{1}) = f(\overline{2}) = f(\overline{3}) = f(\overline{4}) = \overline{0}$, isto é, $f(u) = \overline{0},\ \forall\ u \in \mathbb{Z}_5$. Se F fosse isomorfismo o único elemento de A[X] em correspondência com a função polinomial nula seria o polinômio nulo.

c) O anel $A = \mathbb{Z}_2 \times \mathbb{Z}$ (produto direto) é um anel infinito, comutativo, com unidade, mas não é um anel de integridade. Tomando o polinômio $f = (\overline{1}, 0)X^2 + (\overline{1}, 0)X \in A[X]$ é claro que $f \neq 0$ ($\partial(f) = 2$). Não obstante a função polinomial associada a ele é a função nula pois, $\forall\ (u, v) \in A$,

$$f(u, v) = (\overline{1}, 0)(u^2, v^2) + (\overline{1}, 0)(u, v) = (u^2 + u, 0) = (0, 0).$$

Logo a função F também não é injetora neste caso.

FÓRMULA DE INTERPOLAÇÃO DE LAGRANGE

Teorema 3: Seja K um corpo. Se $a_1, a_2, \ldots, a_n \in K$ são elementos distintos dois a dois e se $b_1, b_2, \ldots, b_n \in K$ ($n > 1$), então existe um polinômio $f \in K[X]$, de grau $n-1$, de maneira que $f(a_1) = b_1, \ldots, f(a_n) = b_n$.

Demonstração: Para cada i ($1 \leqslant i \leqslant n$) consideremos o polinômio

$q_i = (X - a_1) \ldots (X - a_{i-1})(X - a_{i+1}) \ldots (X - a_n)$.

É claro que $q_i(a_j) = 0$, sempre que $j \neq i$, e $q_i(a_i) \neq 0$. Então existe (e pertence a $K[X]$) o polinômio

$$f = \sum_{i=1}^{n} \frac{b_i}{q_i(a_i)}\, q_i = \sum_{i=1}^{n} b_i \left(\prod_{j \neq i} \frac{X - a_j}{a_i - a_j} \right)$$

Calculando, por exemplo, $f(a_1)$, acharemos

$$f(a_1) = \frac{b_1}{q_1(a_1)}\, q_1(a_1) + \ldots + \frac{b_1}{q_n(a_n)}\, q_n(a_1) = b_1$$

Analogamente: $f(a_2) = b_2, \ldots, f(a_n) = b_n$ ■

O polinômio assim construído é chamado *fórmula de interpolação de Lagrange.*

Exemplo: Consideremos o corpo $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. Achemos o polinômio $f \in \mathbb{Z}_5[X]$ tal que $f(\overline{0}) = 1$, $f(\overline{1}) = \overline{2}$ e $f(\overline{2}) = \overline{2}$, dado pela fórmula de Lagrange.

$q_1 = (X - \overline{1})(X - \overline{2}) \Longrightarrow q_1(\overline{0}) = \overline{2}$

$q_2 = (X - \overline{0})(X - \overline{2}) \Longrightarrow q_2(\overline{1}) = -\overline{1} = \overline{4}$

$q_3 = (X - \overline{0})(X - \overline{1}) \Longrightarrow q_3(\overline{2}) = \overline{2}$

Logo

$$f = \frac{1}{2}(X-1)(X-2) + \frac{2}{4}(X-0)(X-2) + \frac{2}{2}(X-0)(X-1) = 3(X^2 - 3X + 2) + 3X(X-2) + X(X-1) = 2X^2 + 4X + 1$$

EXERCÍCIOS

38. Ache a soma dos coeficientes do polinômio:
$f = (1 - 2X + X^4)^2 \cdot (1 + X + X^3)^{240} \in \mathbb{Z}[X]$

Sugestão: a soma dos coeficientes de um polinômio f é f(1).

39. Provar que se um polinômio $f \in A[X]$ é divisível separadamente por $X - a$ e por $X - b$, com $a \in A$ e $b \in A$ e $a \neq b$, então f é divisível por $(X - a)(X - b)$.

Solução

Seja q o quociente da divisão de f por $(X - a)(X - b)$. O resto dessa divisão é $r = mX + n$ pois $\partial(r) < 2$ ou $r = 0$. Temos:

$$f = (X - a)(X - b)q + (mX + n)$$

Como f é divisível por $X - a$, vem:

$$f(a) = (a - a)(a - b)q(a) + (ma + n) = 0 \qquad (1)$$

e, sendo f divisível por $X - b$, vem:

$$f(b) = (b - a)(b - b)q(b) + (mb + n) = 0 \qquad (2)$$

Resolvendo o sistema

$$\begin{cases} ma + n = 0 & (1) \\ mb + n = 0 & (2) \end{cases}$$

nas incógnitas m e n, obtemos $m = n = 0$ e, assim, $r = 0$.

40. Um polinômio f dividido separadamente por $X - 1$, $X + 1$, $X - i$ e $X + i$ dá restos 0, 2, $-5 - 5i$ e $5i - 5$, respectivamente. Obter o resto da divisão de f por $X^4 - 1$, supondo todos esses polinômios em $\mathbb{C}[X]$.

41. Determinar $f \in \mathbb{Z}_7[X]$, com $gr(f) = 5$, satisfazendo as seguintes condições:
$f(\overline{0}) = \overline{1}$, $f(\overline{2}) = \overline{3}$, $f(\overline{3}) = \overline{3}$, $f(\overline{4}) = \overline{6}$ e $f(\overline{5}) = \overline{1}$.

42. Ache $f \in \mathbb{Q}[X]$ tal que $\partial f = 4$; $f(1) = f(-1) = f(2) = f(-2) = 2$ e $f(0) = 6$.

43. Ache $f \in \mathbb{Z}_5[X]$ tal que $\partial f = 3$; $f(\overline{1}) = \overline{0}$; $f(\overline{2}) = \overline{1}$; $f(\overline{3}) = \overline{2}$; $f(\overline{4}) = \overline{3}$.

44. Seja $f \in \mathbb{R}[X]$. Se $u \in \mathbb{C}$ é raiz de f, mostre que $\bar{u}$ é também raiz de f.

45. Seja $f = a_0 + a_1X + \ldots + X^n$ um polinômio em $\mathbb{Z}[X]$. Se $p, q \in \mathbb{Z}$ e $mdc(p, q) = 1$ e, ainda $\frac{p}{q}$ é raiz de f, mostre que $q = \pm 1$ e que $p | a_0$.

46. Se $A = \mathbb{Z}_3$, prove que as funções polinomiais definidas por $f = X$; $g = X^3$; e $h = X + 5X^3 + X^9$ são iguais.

47. Seja $f \in \mathbb{C}[X]$ tal que $f(i) = f(-i) = 2$. Ache o resto da divisão de f por $X^2 + 1$.

48. Mostre que se K é um corpo infinito, então existem funções de K em K não polinomiais.

Solução

Consideremos a aplicação $f: K \longrightarrow K$ tal que $f(0) = 1$ e $f(x) = 0$ para todo $x \in K^*$. Como f admite infinitas raízes em K e f não é nula, então f não pode ser polinomial

49. Mostrar que as funções trigonométricas seno e cosseno não são funções polinomiais.
Sugestão: verifique que $\operatorname{sen} x = 0$ e $\cos x = 0$ têm infinitas raízes.

50. Mostre que se $A = \mathbb{Z}_2 \times \mathbb{Z}$ e se $f \in (\mathbb{Z}_2 \times \mathbb{Z})[X]$ tem grau 2 e $f_A = 0$, então $f = (1, 0)X^2 + (1, 0)X$.

51. Aplique o algorítmo de Briot-Ruffini nos seguintes casos:

i) $f = X^4 - 4X^3 + 5X^2 + 6X - 2$; $g = X - 3$ e $A = \mathbb{Z}$

ii) $f = X^3 + 2X^2$; $g = X + 1$ e $A = \mathbb{Z}_7$.

iii) $f = (1, 0) + (2, 0)X + (3, 0)X^3$; $g = (1, 0) + X$ e $A = \mathbb{Z} \times \{0\}$.

52. Dividir f por g nos seguintes casos:

1º) $f = X^n - 1$ e $g = X - 1$ em $\mathbb{Z}[X]$

2º) $f = X^n + 1$ e $g = X + 1$ em $\mathbb{Z}[X]$

53. Seja K um corpo com n elementos. Provar que o polinômio $X^n - X \in K[X]$ é identicamente nulo, isto é, $u^n - u = 0$, $\forall\, u \in K$.

54. Seja K um corpo finito com n elementos. Se $f \in K[X]$ mostre que:
$f_K = 0 \iff (X^n - X) \mid f$.

55. Seja $K = \{a_1, a_2, \ldots, a_n\}$ um corpo finito com n elementos. Mostre que:
$(X - a_1)(X - a_2) \ldots (X - a_n) = X^n - X$.

56. Seja $K = \{a_1, a_2, \ldots, a_n\}$ um corpo com n elementos.
Sendo $h = (X - a_1) \ldots (X - a_n)$, mostre que $f, g \in K[X]$ determinam a mesma função polinomial se, e somente se, $h \mid (f - g)$.

57. Use a fórmula de interpolação de Lagrange para provar que se K é um corpo finito, então toda função de K em K é uma função polinomial.

§ 4º. — POLINÔMIOS SOBRE UM CORPO

Neste parágrafo somente consideraremos anéis de polinômios sobre um corpo K. Certos resultados que iremos obter aqui poderiam ser conseguidos, às vezes da mesma maneira, em situações mais gerais. Contudo, seja pela sua maior importância nos tópicos que serão aqui tratados, seja por uma questão de uniformidade, nos ateremos aos anéis de polinômios sobre um corpo.*

1. IDEAIS NUM ANEL DE POLINÔMIOS SOBRE UM CORPO

A proposição a seguir dá uma descrição dos ideais de K[X], sempre que K é um corpo.

Proposição 13: Se K é um corpo, então todo ideal em K[X] é principal.

Demonstração: Seja $I \neq <0>$ um ideal em K[X]. Dentre os elementos não nulos de I seja g um polinômio de grau mínimo. É claro que $<g> \subset I$. Mostremos que vale a inclusão contrária.

Dado $f \in I$ o corolário 2 do teorema 1 (deste capítulo) nos assegura que existe um único par de polinômio q, $r \in K[X]$ de maneira que $f = gq + r$, onde $r = 0$ ou $\partial(r) < \partial(g)$. Então $r = f - gq$. Como f e g estão em I, o mesmo acontece com r. Mas não podemos ter $r \in I$ e $\partial(r) < \partial(g)$, do que resulta que só há uma alternativa: $r = 0$. Assim $f = gq$ o que vem mostrar que $f \in <g>$. Ficou provado que $I = <g>$. ■

Corolário: Se K é um corpo, então K[X] é um anel principal.

Demonstração: Já tinhamos visto que se A é um anel de integridade o mesmo acontece com A[X]. É só juntar isso à proposição anterior. ■

2. MÁXIMO DIVISOR COMUM

Conceito: Seja K um corpo. Dados $f, g \in K[X]$, um polinômio $d \in K[X]$ se diz *máximo divisor comum* de f e g se

(i) $d \mid f$ e $d \mid g$

(ii) $(\forall\, d_1 \in K[X])(d_1 \mid f \text{ e } d_1 \mid g \Longrightarrow d_1 \mid d)$

*No capítulo VI veremos uma generalização dos conceitos de máximo divisor comum e de elemento irredutível que serão tratados, nesta altura, para os anéis de polinômios sobre um corpo.

Exemplo: Dados $f = 2 + 2X \in \mathbb{R}[X]$ e $g = 1 - X^2 \in \mathbb{R}[X]$ o polinômio $1 + X$ é máximo divisor comum de f e g. De fato:

(i) $(f = 2d \Longrightarrow d \mid f)$ e $(g = (1 - X)d \Longrightarrow d \mid g)$

(ii) $d_1 \mid f \Longrightarrow \exists\, q \in \mathbb{R}[X]$ tal que $f = d_1 q$. Como $\partial(f) = 1$, então $\partial(d_1) = 0$ ou $\partial(d_1) = 1$.

No primeiro caso $d_1 \in \mathbb{R}^*$ e então a igualdade

$$d = d_1\left(\frac{1}{d_1} + \frac{1}{d_1} X\right)$$

nos mostra que $d_1 \mid d$.

No segundo caso $d_1 = a + bX$ e $q = c$, onde $a, b, c \in \mathbb{R}^*$. Lembrando que $f = d_1 q$ obtemos $ac = bc = 2$. Daí $a = b$ e $d_1 = a(1 + X)$. Portanto

$$d = 1 + X = \frac{1}{a} d_1$$

e que vem mostrar que $d_1 \mid d$.

Proposição 14: Seja K um corpo. Se $f, g \in K[X]$ e se $d \in K[X]$ é um máximo divisor comum de f e g, então um elemento $d' \in K[X]$ será também um máximo divisor comum de f e g se, e somente se, existe $k \in K^*$ tal que $d' = kd$.

Demonstração: ($\Longleftarrow$) Por hipótese $d' = kd$.

(i) $d \mid f \Longrightarrow \exists\, q \in K[X]$ tal que $f = dq$. Como então

$$f = (kd)\left(\frac{1}{k} q\right) = d'\left(\frac{1}{k} q\right)$$

podemos dizer que $d' \mid f$. De maneira análoga se prova que $d' \mid g$.

(ii) $(d_1 \mid f \text{ e } d_1 \mid g) \Longrightarrow d_1 \mid d \Longrightarrow d_1 \mid kd$

($\Longrightarrow$) Se d' é máximo divisor comum de f e g, então $d' \mid f$ e $d' \mid g$. Logo $d' \mid d$. Invertendo o raciocínio chega-se a que $d \mid d'$. Agora:

$d' \mid d \Longrightarrow \exists\ q_1 \in K[X]$ tal que $d = d'q_1$

$d \mid d' \Longrightarrow \exists\ q_2 \in K[X]$ tal que $d' = dq_2$

Donde $d = d(q_1 q_2)$. O caso $d = 0$ só ocorre quando $f = g = 0$ e então $d' = 0$ e qualquer $k \in K^*$ satisfaz a igualdade $d' = kd$. Se $d \neq 0$, então $q_1 q_2 = 1$ e portanto $q_1, q_2 \in K^*$. Fazendo $q_2 = k$ teremos $d' = kd$. ■

Proposição 15: Seja K um corpo. Então, dados $f, g \in K[X]$, existem $h_1, h_2 \in K[X]$ de maneira que o polinômio $d = fh_1 + gh_2$ é um máximo divisor comum de f e g.

Demonstração: Consideremos o ideal $I = \langle f, g \rangle = \{fm_1 + gm_2 \mid m_1, m_2 \in K[X]\}$. Já vimos que todo ideal em K[X] é principal. Logo existe $d \in I$ de maneira que $I = \langle d \rangle$. Mostremos que d é máximo divisor comum de f e g.

(i) $f = f \cdot 1 + g \cdot 0 \Longrightarrow f \in I = \langle d \rangle \Longrightarrow \exists\ q_1 \in K[X]$ tal que $f = dq_1 \Rightarrow d \mid f$.

Um raciocínio análogo nos levará a que $d \mid g$.

(ii) $d \in I \Longrightarrow \exists\ h_1, h_2 \in K[X]$ de modo que $d = fh_1 + gh_2$. Se $d' \in K[X]$ divide f e divide g, a última igualdade nos garante que $d' \mid d$. ■

Nota: O fato de o máximo divisor comum de f e g poder ser representado por $d = fh_1 + gh_2$, nos casos que estamos considerando, é muito importante. Já no item seguinte teremos ocasião de usar tal representação que é conhecida por *identidade de Bezout* com relação aos polinômios f e g em K[X]. O leitor deve se lembrar que acontece uma coisa análoga no caso de máximo divisor comum de números inteiros, conforme foi visto no capítulo zero.

Nota: As duas últimas proposições nos dizem que dois elementos $f, g \in K[X]$ têm tantos máximos divisores comuns quantos são os elementos de K^*. É possível, levando em conta a proposição 14, obter-se a unicidade do máximo divisor comum: é só acrescentar à definição mais um item:

(iii) d é unitário.

Polinômios primos entre si

Dados um corpo K e $f, g \in K[X]$, dizemos que esses polinômios são primos entre si se a unidade de K é um máximo divisor comum de f e g. É claro então que, neste caso, o subconjunto dos elementos de K[X] que satisfazem as condições (i) e (ii) da definição de MDC é K^*, conjunto dos polinômios constantes.

Exemplos

1) Se f é um polinômio constante não nulo e g é um polinômio não nulo qualquer de K[X] então f e g são primos entre si.

2) $f = X + X^2$ e $g = 2 + X + X^2 \in \mathbb{R}[X]$ são primos entre si. Se $p \in \mathbb{R}[X]$ e se $p \mid f$ e $p \mid g$, então $p \mid (g - f)$, isto é $p \mid 2$. Logo f e g só admitem divisores comuns constantes.

Máximo Divisor Comum: Algorítmo

Seja K um corpo e consideremos $f, g \in K[X]$ não nulos. Suponhamos $\partial(f) \geqslant \partial(g)$. Vejamos agora uma maneira prática, pelo menos nos casos em que K é um subcorpo de **C**, para determinar um máximo divisor comum de f e g.

Apliquemos sucessivamente o algorítmo de euclides da seguinte maneira:

$f = gq + r \quad (r = 0 \text{ ou } \partial(r) < \partial(g))$

$g = rq_1 + r_1 \quad (r_1 = 0 \text{ ou } \partial(r_1) < \partial(r))$

$r = r_1 q_2 + r_2 \quad (r_2 = 0 \text{ ou } \partial(r_2) < \partial(r_1))$

$r_1 = r_2 q_3 + r_3 \quad (r_3 = 0 \text{ ou } \partial(r_3) < \partial(r_2))$, etc.

Como não podemos ter $r \neq 0, r_1 \neq 0, r_2 \neq 0, r_3 \neq 0, \ldots$ pois isto acarretaria

$\partial(g) > \partial(r) > \partial(r_1) > \partial(r_2) > \ldots \geqslant 0$ (seqüência infinita)

o que é impossível, então existe um resto r_n dessa seqüência que é nulo e de maneira que os anteriores $r, r_1, \ldots, r_{n-1}$ não são nulos. É claro que está convencionado aí que $r_0 = r$. Afirmamos que r_{n-1} (g no caso n = 0) é um máximo divisor comum de f e g.

Com efeito, temos

$$f = gq + r \quad (\partial(r) < \partial(g))$$
$$g = rq_1 + r_1 \quad (\partial(r_1) < \partial(r))$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$r_{n-3} = r_{n-2}q_{n-1} + r_{n-1} \quad (\partial(r_{n-1}) < \partial(r_{n-2}))$$
$$r_{n-2} = r_{n-1}q_n$$

Como $r_{n-1} \mid r_{n-2}$, devido à última igualdade, então $r_{n-1} \mid r_{n-3}$ (levando em conta a penúltima igualdade). Assim sucessivamente chegamos a que $r_{n-1} \mid g$ e $r_{n-1} \mid f$. Por outro lado, todo divisor de f e g divide r (por causa da primeira igualdade). Se divide g e r divide também r_1. Nessa ordem de idéias chegaremos a que esse polinômio divide também r_{n-1}.

Exemplo: Em $\mathbb{R}[X]$ achemos o máximo divisor comum unitário de $f = 1 + 2X + X^2 + X^3 + X^4$ e $g = 1 + X + X^2 + X^3$.

$f = g \cdot X + (X + 1)$

$g = (X + 1)(X^2 + 1) + 0$

Logo $d = X + 1$ é o m.d.c. procurado.

3. POLINÔMIOS IRREDUTÍVEIS

Conceito: Seja K um corpo. Dizemos que um polinômio $p \in K[X]$ é *irredutível* em K[X] ou irredutível sobre K se

(i) $p \notin K$ (ou seja, p não é polinômio constante);

(ii) Dado $f \in K[X]$, se $f \mid p$, então ou $f \in K^*$ ou existe $c \in K^*$ tal que $f = cp$.

Um polinômio $g \in K[X]$, não constante e não irredutível, chama-se *redutível* ou *composto*.

Exemplos:

1) O polinômio $f = 1 - X^3 \in \mathbb{R}[X]$ é redutível. De fato, além de não ser um polinômio constante ($\partial(f) = 3$), o polinômio $g = 1 - X$ é divisor de f, pois $1 - X^3 = (1 - X)(1 + X + X^2)$, e g não é um polinômio constante e nem pode ser decomposto da maneira $g = c(1 - X^3)$, com $c \in \mathbb{R}^*$.

2) O polinômio $p = 1 + X^2 \in \mathbb{R}[X]$ é irredutível sobre $\mathbb{R}$.

Obviamente p não é um polinômio constante.

Por outro lado, se $f \mid p$, então existe $g \in K[X]$ de maneira que $p = fg$. Como $\partial(p) = 2$, há três alternativas, em princípio, quanto aos graus de f e g: $\partial(f) = \partial(g) = 1$, $\partial(f) = 2$ e $\partial(g) = 0$ e $\partial(f) = 0$ e $\partial(g) = 2$. Mostraremos que a primeira deve ser descartada, restando as duas últimas que correspondem exatamente à conclusão a que devemos chegar quanto à parte (ii) da definição. Vejamos pois que não é possível $\partial(f) = \partial(g) = 1$.

Supondo $f = aX + b$ e $g = cX + d$ $(a, c \neq 0)$, então

$$fg = (aX + b)(cX + d) \Longrightarrow \begin{cases} ac = 1 \\ ad + bc = 0 \\ bd = 1 \end{cases}$$

Multiplicando a segunda dessas igualdades por c e substituindo ac por 1:

$$d + bc^2 = 0$$

Multiplicando esta última relação por d e substituindo bd por 1:

$$d^2 + c^2 = 0$$

Absurdo pois $c \neq 0$.

Nos casos restantes,

- se $\partial(f) = 2$ e $\partial(g) = 0$, então $g = k \in \mathbb{R}^*$ e $f = \frac{1}{k}\, p$,
- se $\partial(f) = 0$, então $f = c \in K^*$.

3) Todo polinômio de grau 1 é irredutível.

Seja $f = aX + b \in K[X]$ um polinômio de grau 1. Então $a \neq 0$ e portanto $f \notin K$. Por outro lado, se $g \mid f$, existe $h \in K[X]$ de modo que

$$f = gh$$

Daí: $1 = \partial(g) + \partial(h)$. Portanto $\partial(g) = 0$ ou $\partial(h) = 0$.

No primeiro caso $g = c \in K^*$.

No segundo, $h = k \in K^*$ e portanto $g = \frac{1}{k}\, f$.

Proposição 16: Seja K um corpo. Se p, f, $g \in K[X]$, p é irredutível, e se $p \mid fg$, então $p \mid f$ ou $p \mid g$.

Demonstração: Suponhamos que p não divide f. Então p e f são primos entre si. Com efeito, pelo fato de p ser irredutível, se $g \mid p$, ou $g = c \in K^*$ ou $g = cp$, com $c \in K^*$. Como nenhum dos polinômios $cp (c \in K^*)$ divide f (em face da hipótese de que p não divide f), concluímos que os divisores comuns a f e p são apenas os polinômios constantes não nulos.

Tomando 1 como máximo divisor comum de f e p, existem $h_1, h_2 \in K[X]$ de maneira que $1 = fh_1 + ph_2$ (identidade de Bezout). Multiplicando por g esta igualdade:

$$g = (fg)h_1 + p(gh_2).$$

Como $p \mid (fg)$ e $p \mid p$, então $p \mid g$. ■

Corolário: Se $p \in K[X]$ é irredutível e $p \mid f_1 f_2 \ldots f_n$, onde cada $f_i \in K[X]$ e $n \geqslant 1$, então p divide um dos f_i.

4. FATORAÇÃO ÚNICA

Recorde-se o teorema fundamental da aritmética: "Todo número natural $n \geqslant 2$ pode ser expresso como um produto de números primos positivos

$$n = p_1 p_2 \ldots p_r \quad (r \geqslant 1)$$

determinados de modo único, a menos de uma permutação". Para todo anel de polinômios sobre um corpo K vale um resultado parecido. É o nosso objetivo seguinte.

Teorema 3: Seja K um corpo e f um polinômio não constante de K[X]. Então existem polinômios irredutíveis $p_1, p_2, \ldots, p_r \in K[X]$ $(r \geqslant 1)$ de maneira que $f = p_1 p_2 \ldots p_r$. Além disso, se $f = q_1 q_2 \ldots q_s$, onde $q_1, q_2, \ldots, q_s \in K[X]$ $(s \geqslant 1)$ são também irredutíveis sobre K, então $r = s$ e cada polinômio p_i é igual ao produto de um polinômio q_j por um elemento conveniente de K^*.

Demonstração

(a) O caso "f irredutível" é imediato. Raciocinemos por indução.

Se $\partial(f) = 1$, f é irredutível conforme já provamos.

Suponhamos $\partial(f) = n > 1$ e que o teorema seja verdadeiro, quanto à decomposição, para todo polinômio de grau r, com $1 \leqslant r < n$.

Admitindo f composto, existem $g, h \in K[X]$ de maneira que $f = gh$ e $0 < \partial(g), \partial(h) < \partial(f)$. Devido à hipótese de indução:

$g = p_1 p_2 \ldots p_t$ e $h = p_{t+1} p_{t+2} \ldots p_r$, onde os p_i são irredutíveis, $t \geqslant 1$ e $r - t \geqslant 1$.

Logo $f = p_1 p_2 \ldots p_r$, nas condições do enunciado.

(b) Vamos supor

$$f = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

Como p_1 é irredutível e $p_1 \mid (q_1 q_2 \cdots q_s)$, então p_1 divide um dos q_j. Supondo que $p_1 \mid q_1$, como q_1 também é irredutível, então existe $c_1 \in K^*$ de maneira que

$$p_1 = c_1 q_1 .$$

Voltando à igualdade do começo e levando em conta a relação que acabamos de obter ficamos com

$$(c_1 q_1) p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

do que resulta

$$(c_1 p_2) p_3 \cdots p_r = q_2 q_3 \cdots q_s .$$

Repetindo sucessivamente o raciocínio desenvolvido acima, até esgotarmos todos os fatores q_j (e conseqüentemente todos os fatores p_i), chegaremos à "unicidade", nos termos do enunciado. ■

5. RAÍZES MÚLTIPLAS

Conceito: Seja K um corpo. Se $f \in K[X]$ e se $u \in K$, já vimos que vale o seguinte resultado: "u é raiz de f $\iff$ $(X - u) \mid f$".

Nessas condições, se q_1 é o quociente na divisão de f por $(X - u)$, então $f = (X - u)q_1$.

Se $q_1(u) \neq 0$ dizemos que u é uma *raiz simples* de f.

Se $q_1(u) = 0$, então q_1 também é divisível por $(X - u)$ e portanto existe $q_2 \in K[X]$ tal que $q_1 = (X - u)q_2$. Donde

$$f = (X - u)^2 q_2 .$$

Se $q_2(u) \neq 0$ dizemos que u é uma *raiz dupla* de f.

Generalizando, se existe um número natural $r \geq 1$ de maneira que

$$f = (X - u)^r q_r \quad e \quad q_r(u) \neq 0$$

dizemos que u é uma *raiz de multiplicidade r* de f.

Uma *raiz múltipla* de f é uma raiz de f cuja multiplicidade é $r > 1$.

Proposição 17: Para que $u \in K$ seja uma raiz múltipla de $f \in K[X]$ é necessário e suficiente que u seja raiz de f' (derivada formal de f).

Demonstração: ($\Longrightarrow$) Se u é raiz múltipla de f, existe $g \in K[X]$ tal que $f = (X - u)^2 g$. Então a derivada de f é dada por

$$f' = 2(X - u)g + (X - u)^2 g' .$$

Portanto $f'(u) = 0$.

($\Longleftarrow$) Admitamos agora que $f(u) = f'(u) = 0$ e que u seja uma raiz simples de f, isto é, $f = (X - u)g$ e $g(u) \neq 0$. Daí

$$f' = (X - u)g' + g$$

e portanto

$$f'(u) = g(u) \neq 0$$

o que é absurdo. ■

Corolário: Se o máximo divisor comum unitário de f e f' é 1, então todas as raízes de f são simples.

Demonstração: Como $mdc(f, f') = 1$, existem $g, h \in K[X]$ tais que $1 = gf + hf'$ (identidade de Bezout). Suponhamos que exista uma raiz múltipla $u \in K$ de f. Então $f(u) = f'(u) = 0$. Daí, achando o valor em u da identidade acima, obtemos

$$1 = g(u)f(u) + h(u)f'(u) = 0$$

o que é absurdo. Assim, com a hipótese feita, todas as raízes de f são simples. ■

Exemplos

1) Seja K um corpo de característica zero ($K = \mathbb{R}$, por exemplo). Então para todo $n \in \mathbb{N}^*$ o polinômio $f = X^n - 1$ só admite raízes simples porque $f' = nX^{n-1} \neq$ polinômio nulo e todas as raízes de f' são nulas ao passo que o zero não é raiz de f. (Onde entrou a hipótese de que a característica de K é zero?).

2) O polinômio $f = 1 + X + X^3$ só admite raízes simples. Achemos o máximo divisor comum de f e $f' = 1 + 3X^2$.

$$3f = f' \cdot X + (2X + 3)$$

$$2f' = (2X + 3)\left(3X - \frac{9}{2}\right) + \frac{31}{2}$$

$$(2X + 3) = \frac{31}{2}\left(\frac{4}{31}X + \frac{6}{31}\right) + 0$$

Como $\frac{31}{2}$ é um máximo divisor comum de f e f', estes polinômios são primos entre si. Daí todas as raízes de f são simples.

6. POLINÔMIOS SOBRE CORPOS ALGEBRICAMENTE FECHADOS

Corpo Algebricamente Fechado

Um corpo K é chamado *algebricamente fechado* se todo polinômio não constante $f \in K[X]$ admite pelo menos uma raiz em K.

Exemplo: O corpo $\mathbb{C}$ dos números complexos é algebricamente fechado: é o que nos garante o "Teorema Fundamental da Álgebra". Existem várias de-

monstrações desse teorema mas não faremos nenhuma delas aqui pois com isso fugiríamos ao escopo deste livro. A primeira demonstração do teorema fundamental da álgebra foi dada por Gauss em 1799. D'Alembert em 1746 foi quem enunciou pela primeira vez tal teorema. Contudo a demonstração por ele apresentada era incorreta.

Contra-exemplos

• O corpo $\mathbb{R}$ dos números reais não é algebricamente fechado. Basta notar que o polinômio $f = 1 + X^2 \in \mathbb{R}[X]$ não tem nenhuma de suas raízes em $\mathbb{R}$. Obviamente se K é um subcorpo de $\mathbb{R}$, como $\mathbb{Z} \subset K$, então $1 + X^2 \in K[X]$ e portanto K também não é algebricamente fechado.

• Um corpo finito não é algebricamente fechado. De fato, seja $K = \{0, 1, a_3, \ldots, a_n\}$ um corpo finito de n elementos. Considerando o polinômio de grau n

$$f = X(X-1)(X-a_3)\ldots(X-a_n)+1 \in K[X]$$

verificamos que $f(u) = 1$, $\forall\, u \in K$. Logo nenhum dos elementos de K é raiz de f.

Proposição 18: Seja K um corpo algebricamente fechado. Dado $f \in K[X]$, então f é irredutível se, e somente se, $\partial(f) = 1$.

Demonstração: Já vimos anteriormente que um polinômio de grau 1 sobre um corpo K é irredutível.

Suponhamos $f \in K[X]$ um polinômio irredutível. Por hipótese existe $u \in K$ de maneira que $f(u) = 0$. Donde $(X - u) \mid f$, o que significa que existe $q \in K[X]$ tal que

$$f = (X-u)q.$$

O fato de que f é irredutível nos leva a concluir que o polinômio q é constante e não nulo, ou seja, $q = a \in K^*$. Portanto

$$f = aX - au$$

é um polinômio de grau 1. ■

Corolário: Seja K um corpo algebricamente fechado. Dado um polinômio não constante $f \in K[X]$, se $\partial(f) = n$, então existem $u_1, u_2, \ldots, u_n \in K$ de maneira que $f = a(X-u_1)(X-u_2)\ldots(X-u_n)$, sendo a o coeficiente dominante e $u_1, u_2, \ldots, u_n$ as raízes de f.

Demonstração: Levando em conta o teorema da fatoração única e a proposição acima podemos decompor f do seguinte modo:

$$f = (a_1X + b_1)(a_2X + b_2)\ldots(a_nX + b_n)$$

onde os a_i são elementos não nulos de K e os $b_i \in K$. Observando que, nessas condições, $a_iX + b_i = a_i(X + \frac{b_i}{a_i})$, $i = 1, 2, \ldots, n$, então

$$(*)\quad f = a_1a_2\ldots a_n(X + \frac{b_1}{a_1})(X + \frac{b_2}{a_2})\ldots(X + \frac{b_n}{a_n}).$$

Como $a_1a_2\ldots a_n = a$ é o coeficiente dominante do segundo membro na igualdade acima, então a é o coeficiente dominante de f. Por outro lado, é claro que se u é uma raiz de f, então u anula um dos fatores $a_iX + b_i$ e portanto $u = -\frac{b_i}{a_i}$. Como, ainda, cada um dos elementos $-\frac{b_i}{a_i}$ é raiz de f, devido à decomposição $(*)$, então o corolário está provado. ■

Nota: Levando em conta a possível existência de raízes múltiplas de f em K o teorema da fatoração única pode ser enunciado, nos casos em consideração, assim: "Todo polinômio não constante f, sobre um corpo K algebricamente fechado, pode ser decomposto, de uma única maneira (salvo permutações dos fatores), da seguinte maneira:

$$f = a(X-u_1)^{k_1}(X-u_2)^{k_2}\ldots(X-u_r)^{k_r}$$

onde $u_i \neq u_j$, sempre que $i \neq j$ $(i, j = 1, 2, \ldots, r)$, os k_i são números naturais não nulos e $k_1 + k_2 + \ldots + k_r = \partial(f)$".

Relações entre coeficientes e raízes

Consideremos um corpo algebricamente fechado K e

$$f = a_0 + a_1X + \ldots + a_nX^n$$

um polinômio de K[X] de grau n.

Se $u_1, u_2, \ldots, u_n \in K$ são as raízes de f, então este polinômio pode ser decomposto da seguinte maneira:

$$f = a_n(X-u_1)(X-u_2)\ldots(X-u_n).$$

Desenvolvendo o produto indicado no segundo membro e levando em conta a condição de igualdade de dois polinômios obtemos:

$$a_{n-1} = -a_n(u_1 + u_2 + \ldots + u_n)$$

$$a_{n-2} = a_n(u_1u_2 + u_1u_3 + \ldots + u_{n-1}u_n)$$

e, de uma maneira geral, observando que o coeficiente de X^{n-k} $(1 \leqslant k \leqslant n)$ é a soma dos produtos

$$(-1)^k u_{i_1}u_{i_2}\ldots u_{i_k}$$

estendida a todas as combinações possíveis $i_1, i_2, \ldots, i_k$ dos n índices $1, 2, \ldots, n$, temos

$$a_{n-k} = (-1)^k a_n \sum u_{i_1}u_{i_2}\ldots u_{i_n}.$$

Em particular

$$a_0 = a_n(-1)^n u_1 u_2 \ldots u_n$$

Se adotarmos as notações

$\sigma_1 = u_1 + u_2 + \ldots + u_n$

. . . . . .

$\sigma_k = \sum u_{i_1} u_{i_2} \ldots u_{i_k}$

. . . . . .

$\sigma_n = u_1 u_2 \ldots u_n$

teremos

$$\frac{a_{n-k}}{a_n} = (-1)^k \sigma_k$$

e portanto

$$f = a_n[X^n - \sigma_1 X^{n-1} + \ldots + (-1)^k \sigma_k X^{n-k} + \ldots + (-1)^n \sigma_n]$$

Exemplos.

1. Polinômios de grau 2

$f = aX^2 + bX + c \in K[X]$ (K algebricamente fechado).

Se u_1 e u_2 indicam as raízes de f em K, então

$$\sigma_1 = u_1 + u_2 = -\frac{b}{a}$$

$$\sigma_2 = u_1 u_2 = \frac{c}{a}$$

e daí

$$f = a(X^2 - \sigma_1 X + \sigma_2)$$

2. Polinômios de grau 3.

$f = aX^3 + bX^2 + cX + d$

Indicando por u_1, u_2 e u_3 as raízes de f (todas em K), temos

$$\sigma_1 = u_1 + u_2 + u_3 = -\frac{b}{a}$$

$$\sigma_2 = u_1 u_2 + u_2 u_3 + u_1 u_3 = \frac{c}{a}$$

$$\sigma_3 = u_1 u_2 u_3 = -\frac{d}{a}$$

e então

$$f = a(X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_3).$$

EXERCÍCIOS

58. Prove, detalhadamente, que o polinômio $d = 5$ é máximo divisor comum de $f = 1 + X^2$ e $g = 1 + X^3$, ambos de $\mathbb{R}[X]$.

59. Determine o máximo divisor comum unitário d dos polinômios f e g de $K[X]$, nos seguintes casos:

a) $f = X^4 - X^2 + \overline{1}$; $g = X^3 + X^2 + X + \overline{1}$; $K = \mathbb{Z}_5$.
b) $f = X^4 + X^3 + X + \overline{1}$; $g = \overline{2}X^3 + \overline{2}X^2 + X + \overline{1}$; $K = \mathbb{Z}_3$.
c) $f = X^4 + X^3 + X + 1$; $g = 2X + 2$; $K = \mathbb{Q}$.

60. Sejam $f, g \in K[X]$ tais que $f \mid g$. Mostre que f é máximo divisor comum entre f e g.

61. Sejam $f, g, q, r \in K[X]$ de modo que $f = g \cdot q + r$. Mostre que se d é máximo divisor comum entre f e g também o é entre g e r.

62. Suponha que o máximo divisor comum unitário de f e $g \in K[X]$ é 1.
Mostre que: $\forall\ h \in K[X]$; $f \mid hg \implies f \mid h$.
Sugestão: use a identidade de Bezout.

63. Seja K um subcorpo do corpo L. Se $f, g \in K[X]$ e $\exists\, u \in L$ tal que $f(u) = g(u) = 0$, mostre que f e g não são primos entre si.

64. Dados $f, g, h \in K[X]$, nenhum deles nulo, mostre que:
a) $mdc(f, g) = 1$ e $mdc(f, h) = 1 \implies mdc(f, gh) = 1$
b) $mdc(f, g) = 1$, $f \mid h$ e $g \mid h \implies fg \mid h$.
Nota: mdc(f, g) indica o máximo divisor comum unitário de f e g.

65. Sejam $p, f, g \in K[X]$ de modo que $mdc(f, g) = 1$. Mostre que p é máximo divisor comum entre pf e pg.

66. Sejam $f, g \in \mathbb{C}[X]$ polinômios não nulos tais que $mdc(f, g) = d$. Provar que $mdc(f^n, g^n) = d^n$ para todo $n > 1$.

67. Determinar todos os mdc de $X^2 + \overline{1}$ e $X^3 + X$ no anel $\mathbb{Z}_3[X]$.

68. Considere o polinômio $f = 4 + 8X^2$.
Como elemento de $\mathbb{Z}[X]$ ele é redutível ou irredutível?
E como elemento de $\mathbb{R}[X]$?
E como elemento de $\mathbb{C}[X]$?
Justifique.

69. Provar que $2 + 2X + X^4 \in \mathbb{Q}[X]$ é irredutível.

70. Prove detalhadamente, que o polinômio $f = 1 + X + X^2$ é irredutível em $\mathbb{R}[X]$.

71. Ache todos os polinômios irredutíveis de grau 2 de $\mathbb{Z}_2[X]$.

72. Seja $f \in K[X]$. Mostre que se $\partial(f) = 2$ ou $\partial(f) = 3$, então ou f admite raiz em K ou é irredutível em $K[X]$ (K corpo.).

73. Mostrar que um polinômio $f \in \mathbb{C}[X]$ é irredutível se, e somente se, $f = aX + b$ onde $a, b \in \mathbb{C}$ e $a \neq 0$.

74. Mostrar que os únicos polinômios irredutíveis de $\mathbb{R}[X]$ são aqueles da forma $aX + b$ $(a \neq 0)$ ou $aX^2 + bX + C$ $(a \neq 0$ e $b^2 - 4ac < 0)$.

75. Decompor em fatores irredutíveis o polinômio $f = X^4 - 4 \in K[X]$ nos seguintes casos: $K = \mathbb{Q}$, $K = \mathbb{R}$, $K = \mathbb{C}$.

76. Mostrar que $X^4 + 4 \in \mathbb{Z}[X]$ é um polinômio composto.

77. Mostrar que $X^2 - 2 \in K[X]$ é irredutível quando $K = \mathbb{Q}$ ou $K = \mathbb{Q}[i]$ mas é redutível sobre $K = \mathbb{Q}[\sqrt{2}]$.

Observação: $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b, \in \mathbb{Q}\}$

$\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}$ e $i =$ unidade imaginária$\}$.

78. Mostrar que $f = X^4 + X^3 + X + 1$ é composto sobre qualquer corpo K.

79. Seja $p \in (K[X] - K)$ tal que " $\forall\, f \in K[X] \implies p \mid f$ ou $mdc(f, p) = 1$".
Mostre que p é irredutível.

80. Seja $p \in (K[X] - K)$ tal que " $\forall\, f, g \in K[X]$, $p \mid fg \implies p \mid f$ ou $p \mid g$".
Mostre que p é irredutível.

81. Sejam $f, g, h \in K[X]$ tais que $f \mid h$ e $g \mid h$ e $mdc(f, g) = 1$. Provar que $fg \mid h$.

82. Sejam $f, g \in K[X]$. Mostrar que $f \mid g$ se, e somente se, g é elemento do ideal gerado por f.

83. Mostrar que se f e g são polinômios divisíveis pelo polinômio h, então r, resto da divisão euclidiana de f por g, também é divisível por h.
Qual é a importância prática deste teorema?
Aplique o teorema na determinação do mdc dos polinômios:
$f = (0, 8, -36, 66, -63, 33, -9, 1, 0, 0, \ldots)$ e
$g = (-8, 28, -38, 25, -8, 1, 0, 0, \ldots)$.

§ 5º — POLINÔMIOS EM DUAS OU MAIS INDETERMINADAS (NOÇÕES)

1. POLINÔMIOS EM DUAS INDETERMINADAS

Já vimos que para todo anel comutativo com unidade A pode-se construir o anel $A[X]$, que também é comutativo com unidade. Logo podemos construir o anel dos polinômios sobre $A[X]$ o qual será indicado por $A[X, Y]$.

Em vista disso deve-se notar que

(i) $A[X, Y] = (A[X])[Y]$

(ii) Um elemento de $A[X, Y]$ é, em princípio, uma seqüência $(f_0, f_1, f_2, \ldots)$ onde $f_i \in A[X]$, $\forall\, i \geqslant 0$, e $\exists\, r \geqslant 0$ de modo que $f_m = 0$, $\forall\, m \geqslant r$

(iii) A adição e a multiplicação em $A[X, Y]$ são definidas, respectivamente, por

$$(f_0, f_1, f_2, \ldots) + (g_0, g_1, g_2, \ldots) = (f_0 + g_0, f_1 + g_1, f_2 + g_2, \ldots)$$

e

$$(f_0, f_1, f_2, \ldots)(g_0, g_1, g_2, \ldots) = (h_0, h_1, h_2, \ldots) \text{ onde } h_k = \sum_{i+j=k} f_i g_j \ (k = 0, 1, \ldots)$$

(iv) $Y = (0, 1, 0, 0, \ldots)$ onde 0 é o polinômio nulo e 1 é o polinômio unidade de $A[X]$.

A notação polinomial de um elemento $F = (f_0, f_1, f_2, \ldots) \in A[X, Y]$ é

$$F = \sum_j f_j Y^j$$

Supondo

$$f_j = \sum_i a_{ij} X^i \ (a_{ij} \in A)$$

teremos

$$F = \sum_i \sum_j a_{ij} X^i Y^j = a_{00} + a_{10} X + a_{01} Y + a_{11} XY \ldots$$

(v) $A[X, Y]$ é também um anel comutativo com unidade. Cada elemento desse anel se denomina *polinômio sobre A nas indeterminadas X e Y.*

(vi) $F = 0$ (pol. nulo) $\iff a_{ij} = 0$, $\forall\, i, j \geqslant 0$

É imediato que: $a_{ij} = 0$ $(\forall\, i, j \geqslant 0) \implies F = 0$

Por outro lado: $F = 0 \implies f_j = 0$ $(\forall\, j \geqslant 0) \implies a_{ij} = 0$, $\forall\, i, j \geqslant 0$.

(vii) Os polinômios constantes de $A[X, Y]$ são os elementos de $A[X]$.

Vejamos um exemplo de como esta última observação pode ser usada. Podemos mostrar que o polinômio $F = X^2 - 2XY + Y^2 \in \mathbb{R}[X, Y]$ é divisível por $Y - X$ usando o corolário do teorema do resto da seguinte maneira:

$$F(X) = X^2 - 2X^2 + X^2 = 0.$$

2. POLINÔMIOS EM n INDETERMINADAS ($n \geqslant 2$)

Dado um anel comutativo com unidade A define-se o anel $A[X_1, \ldots, X_n]$ ($n \geqslant 2$) de polinômios nas n indeterminadas $X_1, \ldots, X_n$, por recorrência, do seguinte modo:

$$A[X_1, \ldots, X_n] = (A[X_1, \ldots, X_{n-1}])[X_n]$$

Temos assim sucessivamente:

$$A[X_1, X_2] = (A[X_1])[X_2], \; A[X_1, X_2, X_3] = (A[X_1, X_2])[X_3], \ldots$$

É claro que X_1 é a indeterminada sobre A, X_2 a indeterminada sobre $A[X_1]$ e assim por diante.

Um elemento típico $F \in A[X_1, \ldots, X_n]$ admite a seguinte representação:

$$F = \sum a_{r_1 r_2 \ldots r_n} X_1^{r_1} X_2^{r_2} \ldots X_n^{r_n}$$

na qual a família dos elementos $a_{r_1 r_2 \ldots r_n}$ é quase nula, ou seja, todos os seus termos são nulos, exceto um número finito deles.

Define-se o *grau* de F, se $F \neq 0$, do seguinte modo: é o maior número natural d com a propriedade:

$$r_1 + r_2 + \ldots + r_n = d \quad \text{e} \quad a_{r_1 r_2 \ldots r_n} \neq 0$$

Notação para o grau de F: $\partial(F)$.

Um polinômio do tipo

$$a_{r_1 r_2 \ldots r_n} X_1^{r_1} X_2^{r_2} \ldots X_n^{r_n}$$

recebe o nome de *monômio*.

Diz-se que um polinômio $F \in A[X_1, X_2, \ldots, X_n]$ é *homogêneo* se todos os seus monômios têm graus iguais.

Exemplo: $F = XY^2 + XYZ + X^2Z - 6Y^2Z \in \mathbb{R}[X, Y, Z]$.

Dado $F \in A[X_1, X_2, \ldots, X_n]$ é sempre possível a seguinte decomposição:

$$F = F_0 + F_1 + F_2 \ldots$$

onde F_0 é homogêneo de grau zero, F_1 é homogêneo de grau um, etc.

A partir dessa decomposição pode-se provar (fica como exercício) que $\forall F, G \in A[X_1, X_2, \ldots, X_n] \Rightarrow \partial(F + G) \leqslant \max\{\partial(F), \partial(G)\}$ e $\partial(FG) \leqslant \partial(F) + \partial(G)$, desde que $F \neq 0, G \neq 0, F + G \neq 0$ e $FG \neq 0$.

Nota: Seja A um anel de integridade. Já vimos então que $A[X]$ também é um anel de integridade e que $U(A[X]) = U(A)$. Por indução pode-se concluir pois que:

- $A[X_1, X_2, \ldots, X_n]$ é um anel de integridade.
- $U(A[X_1, X_2, \ldots, X_n]) = U(A)$

EXERCÍCIOS

84. Escreva na forma de seqüência o seguinte polinômio:
$F = 2 + 2XY + Y^2 \in \mathbb{R}[X, Y]$

85. Escreva com a notação clássica:
$F = (0, 1 + X, X^4, 2X^2, 0, 0, 0, \ldots) \in \mathbb{R}[X, Y]$.

86. Dê o grau do seguinte polinômio, após decompô-lo em polinômios homogêneos:
$F = 2XY + Y^2 + 2XZ^4 + 2ZXY + 4X^2YZ^2 + Z^4 \in \mathbb{Q}[X, Y, Z]$

87. Prove, por indução, que se K é um corpo então $U(K[X_1, \ldots, X_n]) = U(K)$.

88. Seja $F \in K[X, Y]$ (K um corpo). Mostre que se $F(X) = 0$, então $(Y - X) \mid F$.

89. Mostre que se $f \in K[X, Y, Z]$ é divisível por $Y - X$, $Z - X$, $Z - Y$, então f é divisível por $(Y - X) \cdot (Z - X) \cdot (Z - Y)$.

90. Mostre que o polinômio:
$f = X \cdot Y^n + Y \cdot Z^n + Z \cdot X^n - X^n \cdot Y - Y^n \cdot Z - Z^n \cdot X \in \mathbb{R}[X, Y, Z]$ é divisível por $(Y - X) \cdot (Z - X) \cdot (Z - Y)$, $\forall \; n \geqslant 1$.

91. Mostre que $F = (X + Y)^m - X^m - Y^m$ é divisível por $Y + X$ quando m é um número natural ímpar.

92. Dado $F = X^2 + X.Y + Y^2 \in \mathbb{R}[X, Y]$ mostre que não existem $G, H \in \mathbb{R}[X, Y]$ tais que $F = GH$ e $\partial(G),\ \partial(H) > 0$.

93. Seja $F \in \mathbb{R}[X, Y]$ um polinômio simétrico em relação a X e a Y. (Isto quer dizer que permutando X e Y em F obtém-se o próprio F.)
Mostre que: $(Y - X) \mid F \implies (Y - X)^2 \mid F$.

Capítulo V

ANÉIS ORDENADOS

§ 1º — ANÉIS ORDENADOS

1. CONCEITO DE ANEL ORDENADO

Neste capítulo $(A, +, .)$ indicará sempre um anel de integridade. Suporemos ademais que exista uma relação de ordem total sobre o conjunto A e, para indicar que um par ordenado genérico $(x, y) \in A \times A$ pertence a essa relação de ordem, escreveremos apenas $x \leqslant y$.

Definição 1: Dizemos que a relação de ordem considerada é *compatível* com a estrutura de anel de A quando, e apenas quando, os seguintes axiomas se verificam:

(i) $(\forall\ a, b, c \in A)(a \leqslant b \implies a + c \leqslant b + c)$ (compatibilidade com a adição)

(ii) $(\forall\ a, b \in A)(0 \leqslant a \text{ e } 0 \leqslant b \implies 0 \leqslant ab)$ (compatibilidade com a multiplicação).

Um *anel ordenado* é um anel de integridade $(A, +, .)$ tal que no conjunto A existe uma relação de ordem total compatível com a estrutura de anel de A. Dizer que um anel de integridade A é *ordenável* significa que é possível definir uma relação de ordem total sobre A que satisfaça os axiomas (i) e (ii) acima.

Exemplos: Os anéis $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ são anéis ordenados relativamente às relações de ordem usuais respectivas.

2. ALGUNS RESULTADOS SOBRE ANÉIS ORDENADOS

Seja A um anel ordenado. Observemos de início que se $a, b \in A$

$$a < b$$

significa que *a* precede *b* (na relação considerada) e que $a \neq b$. Dizemos que a *precede estritamente* b para significar que $a < b$.

Proposição 1: Seja A um anel ordenado. Então, para a, b, c e A quaisquer, vale o seguinte:

(a) $a \leqslant b \iff a + c \leqslant b + c$

(b) $a < b \iff a + c < b + c$

Demonstração: (a) ($\Longrightarrow$) Vale por definição de anel ordenado.
($\Longleftarrow$) $a + c \leqslant b + c \Longrightarrow (a + c) + (-c) \leqslant (b + c) + (-c) \Longrightarrow a + (c + (-c)) \leqslant b + (c + (-c)) \Longrightarrow a + 0 \leqslant b + 0 \Longrightarrow a \leqslant b$.

(b) ($\Longrightarrow$) $a < b \Longrightarrow a + c \leqslant b + c$, por definição. Se tivéssemos $a + c = b + c$, então $a = b$, o que seria contrário à hipótese. Logo $a + c \neq b + c$. Portanto $a + c < b + c$.

($\Longleftarrow$) $a + c < b + c \Longrightarrow a \leqslant b$, devido à parte (a). Se pudesse acontecer a igualdade $a = b$, teríamos também $a + c = b + c$, o que não é possível. Logo $a \neq b$. Donde $a < b$. ■

Corolário 1: Num anel ordenado A são equivalentes as seguintes afirmações: (a) $x \leqslant y$, (b) $0 \leqslant y - x$ e (c) $-y \leqslant -x$.

Demonstração: (a) $\Longrightarrow$ (b)

$x \leqslant y \Longrightarrow x + (-x) \leqslant y + (-x) \Longrightarrow 0 \leqslant y - x$

(b) $\Longrightarrow$ (c)

$0 \leqslant y - x \Longrightarrow (-y) + 0 \leqslant (-y) + (y - x) \Longrightarrow -y \leqslant -x$

(c) $\Longrightarrow$ (a)

$-y \leqslant -x \Longrightarrow y + (-y) \leqslant y + (-x) \Longrightarrow 0 \leqslant y + (-x) \Longrightarrow x + 0 \leqslant x + (y + (-x)) \Rightarrow x \leqslant y$. ■

Corolário 2: Num anel ordenado são equivalentes as afirmações: (a) $x < y$, (b) $0 < y - x$ e (c) $-y < -x$.

Deixamos a demonstração deste corolário como exercício.

Proposição 2: ("Adição de desigualdades"): Seja A um anel ordenado. Se $x_1, \ldots, x_n, y_1, \ldots, y_n \in A$ $(n \geqslant 2)$ e se $x_i \leqslant y_i$ $(i = 1, \ldots, n)$, então

$$x_1 + \ldots + x_n \leqslant y_1 + \ldots + y_n .$$

Se, além das hipóteses já feitas, existir um índice $r (1 \leqslant r \leqslant n)$ de modo que $x_r < y_r$, então

$$x_1 + \ldots + x_n < y_1 + \ldots + y_n$$

Demonstração: Façamos a demonstração para $n = 2$. Para generalizar depois é só raciocinar por indução.

$$\left.\begin{array}{l} x_1 \leqslant y_1 \Longrightarrow x_1 + x_2 \leqslant y_1 + x_2 \\ x_2 \leqslant y_2 \Longrightarrow x_2 + y_1 \leqslant y_2 + y_1 \end{array}\right\} \Longrightarrow \quad x_1 + x_2 \leqslant y_1 + y_2$$

Suponhamos agora, por exemplo, que se tenha $x_1 < y_1$ e $x_2 \leqslant y_2$. De acordo com a dedução acima temos que

$$x_1 + x_2 \leqslant y_1 + y_2 .$$

De $x_1 < y_1$ resulta que $x_1 + x_2 < y_1 + x_2$. Portanto, se valesse a igualdade $x_1 + x_2 = y_1 + y_2$, teríamos em conseqüência $y_1 + y_2 < y_1 + x_2$. Daí então $y_2 < x_2$ o que é absurdo já que, por hipótese, $x_2 \leqslant y_2$. Consequentemente

$$x_1 < y_1 \text{ e } x_2 \leqslant y_2 \Longrightarrow x_1 + x_2 < y_1 + y_2 . \quad ■$$

Proposição 3: Sejam a, b e c elementos genéricos de um anel ordenado A. Então:

(i) $a \leqslant b$ e $0 \leqslant c \Longrightarrow ac \leqslant bc$

(ii) $a \leqslant b$ e $c \leqslant 0 \Longrightarrow bc \leqslant ac$

(iii) $a < b$ e $0 < c \Longrightarrow ac < bc$

(iv) $a < b$ e $c < 0 \Longrightarrow bc < ac$

Demonstração:

(i) $a \leqslant b \Longrightarrow 0 \leqslant b - a \Longrightarrow 0 \leqslant (b - a)c \Longrightarrow 0 \leqslant bc - ac \Longrightarrow ac \leqslant bc$

(ii) Fica como exercício

(iii) Exercício

(iv) $a < b$ e $c < 0 \Longrightarrow bc \leqslant ac$, isto em virtude da parte (ii) desta proposição. Supondo $bc = ac$, como A é um anel de integridade e como $c \neq 0$, então $b = a$ o que é contrário à hipótese. Logo $bc \neq ac$. Das conclusões obtidas segue que $bc < ac$. ■

Corolário 1 ("Regras de Sinais"): Sejam *a* e *b* elementos genéricos de um anel ordenado A. Então:

(i) $0 < a \text{ e } 0 < b \implies 0 < ab$

(ii) $0 < a \text{ e } b < 0 \implies ab < 0$

(iii) $a < 0 \text{ e } b < 0 \implies 0 < ab$.

Demonstração:

(i) $0 < a \text{ e } 0 < b \Rightarrow 0 \cdot b < ab$, em conseqüência da terceira parte da proposição. Ou seja: $0 < ab$.

(ii) e (iii) Ficam como exercício as demonstrações. ■

Corolário 2: Seja A um anel ordenado. Então:

(i) $\forall\, a \in A \implies 0 \leqslant a^2$

(ii) $(\forall\, a \in A)(a \neq 0 \implies 0 < a^2)$

(iii) $0 < 1_A$.

Demonstração:

(i) Como A é totalmente ordenado só há duas alternativas: $0 \leqslant a$ ou $a \leqslant 0$. No primeiro caso a primeira parte da proposição nos assegura que

$$0 \cdot a \leqslant aa$$

ou seja,

$$0 \leqslant a^2.$$

No segundo caso procede-se de maneira análoga.

(ii) No caso $a \neq 0$ não se pode ter $a^2 = 0$ pois A é anel de integridade. Logo, levando em conta a primeira parte, o que se tem é o seguinte: $0 \leqslant a^2$ e $a^2 \neq 0$. Ou seja: $0 < a^2$.

(iii) É um caso particular da parte anterior. É só lembrar que $1_A \neq 0$ e que $1_A^2 = 1_A$. ■

Aplicação: O anel $\mathbb{C}$ dos complexos não é ordenável.

Suponhamos que fosse. Então existiria uma relação de ordem total sobre $\mathbb{C}$ para a qual valeriam simultâneamente as desigualdades

$$0 < i^2 \text{ e } 0 < 1$$

onde i é a unidade imaginária. Daí

$$0 < -1 \text{ e } 0 < 1$$

ou, equivalentemente,

$$1 < 0 \text{ e } 0 < 1$$

o que é impossível.

3. VALOR ABSOLUTO

Seja a um elemento de um anel ordenado A. Indica-se então por $|a|$ o *valor absoluto* de a, cuja definição é a seguinte:

$|a| = a$, se $0 \leqslant a$ e

$|a| = -a$, quando $a < 0$.

É imediato então que $|a| = |-a|$, $\forall\, a \in A$.

Proposição 4: Sejam *a* e *b* elementos de um anel ordenado A. Então:

(i) $-|a| \leqslant a \leqslant |a|$

(ii) $|ab| = |a|\,|b|$

(iii) $|a + b| \leqslant |a| + |b|$

(iv) $|a| - |b| \leqslant |a - b| \leqslant |a| + |b|$

Demonstração: Quando $a = 0$ ou $b = 0$ as afirmações da proposição são imediatas. Portanto admitamos $a \neq 0$ e $b \neq 0$.

(i) $0 < a \implies |a| = a$ e $-|a| = -a$. Mas $0 < a \implies -a < 0$. Logo $-a < a$. Assim

$$-a = -|a| < a = |a|.$$

$a < 0 \implies |a| = -a$ e $-|a| = a$. Mas $a < 0 \implies 0 < -a$. Logo $a < -a$. Portanto

$$-|a| = a < -a = |a|$$

(ii) $0 < a \text{ e } 0 < b \implies 0 < ab$. Logo, neste caso, $|a|\,|b| = ab$ e $|ab| = ab$.

$a < 0 \text{ e } b < 0 \implies 0 < ab$. Aqui temos então $|a|\,|b| = (-a)(-b) = ab$ e $|ab| = ab$.

$a < 0 \text{ e } 0 < b \implies ab < 0$. Portanto $|a|\,|b| = (-a)b = -(ab)$ e $|ab| = -(ab)$.

É análoga ao anterior o caso em que $0 < a \text{ e } b < 0$.

(iii) Levando em conta que

$$-|a| \leqslant a \leqslant |a| \quad \text{e} \quad -|b| \leqslant b \leqslant |b|$$

obtemos, por meio da proposição 2 (adição de desigualdades):

$$-(|a| + |b|) \leqslant a + b \leqslant |a| + |b|$$

No caso $|a + b| = a + b$ é uma conclusão direta que $|a + b| \leqslant |a| + |b|$. Se, ao contrário, $|a + b| = -(a + b)$, então $-(|a| + |b|) \leqslant -|a + b|$. Logo $|a + b| \leqslant |a| + |b|$ também para esta última possibilidade.

(iv) Como $a = (a - b) + b$ a parte (iii) acima nos diz que

$$|a| \leqslant |a - b| + |b|$$

e daí

$$|a| - |b| \leqslant |a - b|$$

Por outro lado, como $a - b = a + (-b)$, então

$$|a - b| \leqslant |a| + |-b| = |a| + |b|$$

Das duas últimas conclusões tiramos então a tese

$$|a| - |b| \leqslant |a - b| \leqslant |a| + |b|. \quad \blacksquare$$

4. ELEMENTOS POSITIVOS E ELEMENTOS NEGATIVOS

Dado um anel A, se L é um subconjunto não vazio de A, definimos a *soma* de L com L, o *produto* de L por L e o *oposto* de L, respectivamente, por

$$L + L = \{x + y \mid x, y \in L\}$$

$$LL = \{xy \mid x, y \in L\}$$

$$-L = \{-x \mid x \in L\}$$

Isto posto, é claro que $L + L \subset L$ significa que L é fechado para a adição de A e $LL \subset L$ que L é fechado para a multiplicação de L.

Proposição 5: Seja A um anel ordenado. Se $P = \{x \in A \mid 0 \leqslant x\}$, então (i) $P + P \subset P$; (ii) $PP \subset P$; (iii) $P \cup (-P) = A$ e (iv) $P \cap (-P) = \{0\}$. Reciprocamente, se A é um anel de integridade e se existe um subconjunto não vazio $P \subset A$ de maneira que as condições (i), (ii), (iii) e (iv) acima se verifiquem, então A é ordenável.

Demonstração: $(\Longrightarrow)$

(i) $x, y \in P \Longrightarrow 0 \leqslant x$ e $0 \leqslant y \Longrightarrow 0 \leqslant x$ e $0 + x \leqslant y + x \Longrightarrow 0 \leqslant x + y \Longrightarrow x + y \in P$

(ii) $x, y \in P \Longrightarrow 0 \leqslant x$ e $0 \leqslant y \Longrightarrow 0 \leqslant xy \Longrightarrow xy \in P$

(iii) Seja x um elemento do anel A. Como a relação de ordem considerada sobre A é total, então

$$0 \leqslant x \quad \text{ou} \quad x \leqslant 0$$

Mas

$$x \leqslant 0 \Longrightarrow (-x) + x \leqslant 0 + (-x) \Longrightarrow 0 \leqslant -x \Longrightarrow -x \in P \Longrightarrow x \in (-P).$$

Logo, ou $x \in P$ ou $x \in (-P)$.

Assim ficou provado que $A \subset P \cup (-P)$. Como obviamente $P \cup (-P) \subset A$, então $A = P \cup (-P)$.

(iv) $x \in P \cap (-P) \Longrightarrow 0 \leqslant x$ e $0 \leqslant -x \Longrightarrow 0 \leqslant x$ e $x + 0 \leqslant x + (-x)$ $0 \leqslant x$ e $x \leqslant 0 \Longrightarrow x = 0$. Logo $P \cap (-P) = \{0\}$.

$(\Longleftarrow)$ Por hipótese agora existe um subconjunto não vazio $P \subset A$ que satisfaz (i), (ii), (iii) e (iv). Dados a, b $\in$ A, elementos genéricos, ponhamos por definição

$$a \leqslant b \iff b - a \in P.$$

Mostremos então que a relação assim definida é uma relação de ordem compatível com a estrutura de anel de A.

- $0 \in P \Rightarrow a - a \in P, \forall\, a \in A \Rightarrow a \leqslant a, \forall\, a \in A.$
- $a \leqslant b$ e $b \leqslant a \Longrightarrow b - a \in P$ e $a - b \in P \Longrightarrow b - a \in P$ e $b - a = -(a - b) \in (-P) \Longrightarrow b - a = 0 \Longrightarrow a = b$
- $a \leqslant b$ e $b \leqslant c \Longrightarrow b - a \in P$ e $c - b \in P \Longrightarrow (b - a) + (c - b) = c - a \in P \Longrightarrow a \leqslant c.$
- $\forall\, a, b \in A \Longrightarrow b - a \in A \Longrightarrow b - a \in P$ ou $b - a \in (-P) \Longrightarrow b - a \in P$ ou $a - b \in P \Longrightarrow a \leqslant b$ ou $b \leqslant a.$
- $\forall\, a, b, c \in A$:

$a \leqslant b \Longrightarrow b - a \in P \Longrightarrow b + c - a - c \in P \Longrightarrow (b + c) - (a + c) \in P \Longrightarrow a + c \leqslant b + c$

- $\forall\, a, b \in A$:

$0 \leqslant a$ e $0 \leqslant b \Longrightarrow a, b \in P \Longrightarrow ab \in P \Longrightarrow 0 \leqslant ab.$ $\blacksquare$

Nota: A proposição acima nos garante que um anel de integridade A é ordenável de tantas maneiras quantos forem os subconjuntos $P \subset A$, $P \neq \phi$, que satisfaçam (i), (ii), (iii) e (iv). Inclusive, se não existir nenhum subconjunto não vazio $P \subset A$, com as condições exigidas na proposição, pode-se dizer que A não é ordenável.

Definição 2: Seja A um anel ordenável. Se $P = \{x \in A \mid 0 \leqslant x\}$, os elementos de P são chamados *elementos positivos* do anel e os de $(-P)$ são os *elementos negativos* de A. Um elemento de P que é diferente do zero de A se diz *estritamente positivo*; os elementos não nulos de $(-P)$ são os elementos *estritamente negativos* do anel.

Exemplos:

1) No anel $\mathbb{Z}$ dos inteiros o conjunto $\mathbb{Z}_+ = \{0, 1, 2, \ldots\}$ verifica as condições (i), (ii), (iii) e (iv) da proposição. A relação de ordem daí resultante é a usual. Mostraremos que não há nenhuma outra relação de ordem total sobre $\mathbb{Z}$ que seja compatível com a estrutura de anel de $\mathbb{Z}$.

Suponhamos que houvesse e seja P o conjunto dos elementos positivos para essa outra relação de ordem. Portanto $0, 1 \in P$. Daí

$$1 + 1, 1 + 1 + 1, \ldots \in P.$$

Isso tudo nos garante então que $\mathbb{Z}_+ \subset P$.

Admitamos agora que pudesse existir $n \in P$ de maneira tal que $n \notin \mathbb{Z}_+$. Então $n \neq 0$ e $-n \notin \mathbb{Z}_+$. Como $\mathbb{Z}_+ \subset P$, segue que $-n \in P$. Donde $n \in (-P)$. Levando em conta que $P \cap (-P) = \{0\}$ a conclusão é que $n = 0$. Absurdo.

2) No anel $\mathbb{Q}$ dos racionais o conjunto $\mathbb{Q}_+ = \{\frac{a}{b} \in \mathbb{Q} \mid ab \in \mathbb{Z}_+\}$ verifica as condições exigidas na proposição 5. A relação de ordem associada a $\mathbb{Q}_+$ é a usual sobre $\mathbb{Q}$.

Suponhamos que houvesse uma outra relação de ordem sobre $\mathbb{Q}$, compatível com a estrutura de anel de $\mathbb{Q}$, e chamemos de P o conjunto dos elementos positivos com respeito a esta última. Do mesmo modo que foi feito no exemplo anterior pode-se concluir então que

$$\mathbb{Z}_+ \subset P$$

Tomemos $\frac{a}{b} \in \mathbb{Q}_+$, $\frac{a}{b} \neq 0$. Então $ab^{-1}\, b^2 \in \mathbb{Z}_+$, ou seja, $ab = ab^{-1}\, b^2 \in P$. Mas $b^2 \neq 0$ e $b^2 \in P$. Podemos então concluir que $ab^{-1} \in P$. De fato: $ab^{-1} \in (-P) \Rightarrow$ $\Rightarrow -(ab^{-1}) \in P \Rightarrow -(ab^{-1})b^2 \in P \Rightarrow -ab \in P \Rightarrow ab \in (-P)$ (absurdo).

Ficou assim provado que $\mathbb{Q}_+ \subset$ P. Repetindo a argumentação usada no exemplo anterior prova-se que $P \subset \mathbb{Q}_+$.

3) Consideremos o anel $A = \mathbb{R}[X]$. Seja $P = \{f \in A \mid f = 0$ ou $cd(f) > 0\}$, onde $cd(f)$ indica o coeficiente dominante de f. Mostremos que P satisfaz as condições da proposição 5.

(i) Sejam $f, g \in P$. Indiquemos por p e q os coeficientes dominantes respectivos. É claro que se $f = 0$ ou $g = 0$ ou $f + g = 0$, a soma $f + g$ pertence a P. Caso contrário, $cd(f+g) = p$ ou $cd(f+g) = q$ ou $cd(f+g) = p+q$. Donde $f+g$ também pertence a P.

(ii) É claro também que se $f = 0$ ou $g = 0$, então $fg = 0 \in P$. Supondo $f \neq 0$ e $g \neq 0$, então $fg \neq 0$ e $cd(fg) = cd(f)cd(g) = pq > 0$, ou seja, $fg \in P$.

(iii) Dado $f \in A$, só há três alternativas: $f = 0$, $cd(f) > 0$ ou $cd(f) < 0$ (cada uma excluindo as demais). Logo $f \in P$ ou $f \in (-P)$.

(iv) Seja $f \in P \cap (-P)$. Suponhamos $f \neq 0$. Então $cd(f) > 0$ e $cd(-f) = -cd(f) > 0$. Donde $cd(f) > 0$ e $cd(f) < 0$. Absurdo.

Por exemplo, em relação a ordem assim determinada, podemos dizer que, se $f = 1 + 4X^{10}$ e $g = X^{15}$, então $f < g$, uma vez que

$$g - f = -1 - 4X^{10} + X^{15}$$

tem coeficiente dominante maior que zero.

Nota: Essa não é a única maneira de ordenar o anel $\mathbb{R}[X]$. De fato, dado um polinômio $f = a_0 + a_1 X + \ldots + a_n X^n \neq 0$, chamemos de *coeficiente inicial* de f o primeiro de seus coeficientes não nulos (na ordem $a_0, a_1, \ldots$). Denotemos esse coeficiente inicial por $ci(f)$.

Nessas condições o conjunto $P_1 = \{f \in \mathbb{R}[X] \mid f = 0$ ou $ci(f) > 0\}$ também verifica as condições exigidas na proposição 5. Deixamos ao leitor como exercício a constatação desse fato.

5. ANÉIS BEM ORDENADOS — ANÉIS ARQUIMEDIANOS

Definição 3: Seja A um anel ordenado. Dizemos que A é um *anel bem ordenado* se todo subconjunto de P (conjunto dos elementos positivos do anel) possui mínimo.

Exemplo: O anel $\mathbb{Z}$ é bem ordenado. O princípio do menor número inteiro nos garante que todo subconjunto de $\mathbb{Z}_+ = \{0, 1, 2, \ldots\}$ admite um menor elemento.

Contra-exemplo: O anel $\mathbb{Q}$ não é bem ordenado. O subconjunto $L = \{x \in \mathbb{Q} \mid 0 < x < 1\}$, por exemplo, está contido em $\mathbb{Q}_+$ e no entanto não existe o mínimo de L. Com efeito, dado $a \in L$, é claro que $\frac{a}{2} < a$ e $\frac{a}{2} \in L$.

Proposição 6: Seja A um anel bem ordenado. Então não existe $x \in A$ de maneira que $0 < x < 1$ (1 = unidade de A).

Demonstração: Suponhamos que exista $a \in A$ de modo que $0 < a < 1$. Então $L = \{x \in A \mid 0 < x < 1\} \neq \phi$ e $L \subset P$. Seja m o mínimo de L. Como $m \in L$, então $0 < m < 1$. Daí (multiplicando por m):

$$0 < m^2 < m.$$

Como $m < 1$, temos então

$$0 < m^2 < m < 1$$

o que nos diz que $m^2 \in L$ e $m^2 < m$. Absurdo. ∎

Definição 4: Um anel ordenado A se diz *arquimediano* se, para todo $a \in A$, existe $n \in \mathbb{N}^*$, de maneira que $n1_A = 1_A + 1_A + \ldots + 1_A > a$ (o número de parcelas, obviamente é n).

Exemplo: O anel $\mathbb{Z}$ é arquimediano. Dado $a \in \mathbb{Z}$, é claro que fazendo $|a| = m$, então $(m+1).1 > a$.

Contra-exemplo: O anel $\mathbb{R}[X]$ com a relação de ordem fornecida por $P = \{f \in \mathbb{R}[X] \mid f = 0 \text{ ou } cd(f) > 0\}$ não é arquimediano.

De fato, dado por exemplo $f = X^2$, como para todo $n \in \mathbb{N}^*$,

$$cd(f - n \cdot 1) = cd(X^2 - n) = 1 > 0,$$

então $n \cdot 1 = n < f$, $\forall\, n \in \mathbb{N}^*$.

Proposição 7: Todo anel de integridade bem ordenado é arquimediano.

Demonstração: Seja A um anel bem ordenado. Se A não fosse arquimediano existiria um elemento $a \in A$ de modo que

$$n1_A \leqslant a, \quad \forall\, n \in \mathbb{N}^*.$$

Seja $L = \{a - n1_A \mid n \in \mathbb{N}^*\}$. Por hipótese L só possui elementos positivos, isto é, $L \subset P$. Seja $a - r1_A$ o mínimo de L. Observemos que o elemento $a - (r+1)1_A \in L$. Além disso

$$-1_A < 0 \Longrightarrow -r1_A - 1_A < -r1_A \Longrightarrow -(r+1)1_A < -r1_A \Longrightarrow a - (r+1)1_A < a - r1_A$$

Contradição com o fato de $a - r1_A$ ser o mínimo de L. Portanto A é arquimediano. ■

Nota: A recíproca da proposição acima não é verdadeira. O anel $\mathbb{Q}$, por exemplo, é arquimediano mas não é bem ordenado.

6. CARACTERÍSTICA DE UM ANEL ORDENADO

Proposição 8: A característica de um anel ordenado A é zero.

Demonstração: Já vimos que $0 < 1_A$. Logo $0 + 1_A < 1_A + 1_A$, ou seja, $1_A < 2 \cdot 1_A$. Raciocinando por indução iremos concluir que

$$0 < n1_A, \quad \forall\, n \in \mathbb{N}^*.$$

Logo $n1_A \neq 0$, $\forall\, n \in \mathbb{N}^*$. Donde $c(A) = 0$. ■

Corolário: Um anel finito não é ordenável.

Demonstração: É só lembrar que a característica de um anel finito é maior que zero. ■

§ 2º — CORPO ORDENADO

1. CONCEITO DE UM CORPO ORDENADO

Seja $(K, +, \cdot)$ um corpo. Se, como anel de integridade que é, K for um anel ordenado, diremos então que K é um *corpo ordenado*. Dizer que um corpo K é *ordenável* significa que é possível definir uma relação de ordem total sobre K, relação essa compatível com a estrutura de anel de K.

Exemplos: Os corpos $\mathbb{Q}$ e $\mathbb{R}$ são corpos ordenados. O corpo $\mathbb{C}$ dos complexos não é ordenável.

Nota: É uma conseqüência imediata da definição acima que todas as propriedades de um anel ordenado são válidas para os corpos ordenados. Inclusive, para que um corpo K seja ordenável, é necessário e suficiente que exista um subconjunto não vazio $P \subset K$, de maneira que

$$P + P \subset P,\ PP \subset P,\ P \cup (-P) = K \text{ e } P \cap (-P) = \{0\}.$$

Proposição 8: Sejam a e b elementos quaisquer de um corpo ordenado K. Então: (a) $(0 < a \Longrightarrow 0 < a^{-1})$ e $(a < 0 \Longrightarrow a^{-1} < 0)$;

(b) $(0 < a < 1_A \Longrightarrow 1_A < a^{-1})$ e $(1_A < a \Longrightarrow 0 < a^{-1} < 1_A)$;

(c) $0 < a < b \Longrightarrow b^{-1} < a^{-1}$

(d) $a < b < 0 \Longrightarrow b^{-1} < a^{-1} < 0$

Demonstração:

(a) $0 < a \Longrightarrow a \neq 0 \Longrightarrow a^{-1} \neq 0 \Longrightarrow 0 < (a^{-1})^2$. Multiplicando a desigualdade inicial por $(a^{-1})^2$ obtemos

$$0 \cdot (a^{-1})^2 < a(a^{-1})^2$$

ou seja, que $0 < a^{-1}$.

Deixamos o término da demonstração a cargo do leitor.

(b) $0 < a \Longrightarrow 0 < a^{-1}$, conforme parte (a) da demonstração. Multiplicando $0 < a < 1_A$ por a^{-1} obtemos

$$0 < 1_A < a^{-1}$$

Fica como exercício o restante da demonstração desta parte.

(c) $0 < a < b \implies 0 < a^{-1}$ e $0 < b^{-1} \implies 0 < a^{-1}b^{-1}$.

Multiplicando $0 < a < b$ por $a^{-1}b^{-1}$ obtemos

$$0 < b^{-1} < a^{-1}.$$

(d) Exercício. ■

Proposição 9: Seja a um elemento não nulo de um corpo ordenado K. Então $|a^{-1}| = |a|^{-1}$ e, em particular, $|ab^{-1}| = |a||b|^{-1}$, para todo elemento $b \in K$, $b \neq 0$.

Demonstração: Como $|a^{-1}||a| = |a^{-1}a| = |1_A| = 1_A$, então $|a^{-1}| = |a|^{-1}$. Daí

$$|ab^{-1}| = |a||b^{-1}| = |a||b|^{-1}.$$

Usando a notação de quocientes o resultado obtido por último se traduz em

$$\left|\frac{a}{b}\right| = \frac{|a|}{|b|}$$ ■

Proposição 10: Sejam a e b elementos de um corpo ordenado K tais que $a < b$. Então existe um elemento $c \in K$, de maneira que $a < c < b$.

Demonstração: Como $0 < 1_A$, então $0 < 2 \cdot 1_A$, e, portanto, $0 < (2 \cdot 1_A)^{-1}$. Por outro lado

$$a < b \implies \begin{cases} a + a < a + b \implies a(2 \cdot 1_A) < a + b \\ \text{e} \\ a + b < b + b \implies a + b < b(2 \cdot 1_A). \end{cases}$$

Multiplicando as duas últimas desigualdades obtidas por $(2 \cdot 1_A)^{-1}$ o resultado é o seguinte:

$$a < (a + b)(2 \cdot 1_A)^{-1} \quad \text{e}$$
$$(a + b)(2 \cdot 1_A)^{-1} < b.$$

Portanto

$$a < (a + b)(2 \cdot 1_A)^{-1} < b.$$

O elemento $c = (a + b)(2 \cdot 1_A)^{-1}$ satisfaz então a afirmação do enunciado. ■

EXERCÍCIOS

1. Seja A um anel ordenado. Mostre que:

a) se $a, p \in A$ e $0 < p$, então $a - p < a$

b) $0 < a \cdot c$ e $0 < c \implies 0 < a$

c) $b < a$ e $c < 0 \implies a \cdot c < b \cdot c$

d) $0 < a \cdot c$ e $c < 0 \implies a < 0$

e) $0 < b_1 < a_1$ e $0 < b_2 < a_2 \implies b_1 \cdot b_2 < a_1 \cdot a_2$

f) $b_1 < a_1$ e $b_2 < a_2 \implies a_1 \cdot b_2 + a_2 \cdot b_1 < a_1 \cdot a_2 + b_1 \cdot b_2$

g) $2 \cdot a \cdot b \leqslant a^2 + b^2, \forall\, a, b \in A$

h) $0 < a^2 + a \cdot b + b^2, \forall\, a, b \in A,\ a \neq 0$ ou $b \neq 0$

Solução

a) $0 < p \Rightarrow -p < 0$

Somando aos dois membros da última desigualdade temos $a - p < a$.

b) Não podemos ter $a = 0$ pois isto implicaria $ac = 0$. Por outro lado, se tivéssemos $a < 0$, como $0 < c$, as regras de sinais aplicadas a este caso nos dariam $ac < 0$ o que é impossível. Logo $0 < a$.

e) De $b_1 < a_1$ e $0 < b_2$ decorre $b_1 b_2 < a_1 b_2$. De $b_2 < a_2$ e $0 < a_1$ segue $b_2 a_1 < a_2 a_1$. Donde $b_1 b_2 < a_1 a_2$.

h) São imediatos os casos em que $a = 0$ e $b \neq 0$ ou $a \neq 0$ e $b = 0$.

Suponhamos pois $a \neq 0$ e $b \neq 0$. Daí $a^2 > 0$ e $b^2 > 0$. Se $a > 0$ e $b > 0$ (ou $a < 0$ e $b < 0$), então $ab > 0$ e portanto $a^2 + b^2 + ab > 0$.

Se $a < 0$ e $b > 0$ (ou $a > 0$ e $b < 0$), então $ab < 0$ e daí $|ab| = -ab$.

Temos então: $a^2 + ab + b^2 = a^2 - |ab| + b^2 = a^2 - 2|ab| + b^2 + |ab| = (|a| - |b|)^2 + |ab| > 0$.

2. Prove por indução os seguintes propriedades num anel ordenado A:

a) $0 < a \implies 0 < a^n, \quad \forall\ n \in \mathbb{N}$

b) $a < 0 \implies 0 < a^{2n}, \quad \forall\ n \in \mathbb{N}$

c) $a < 0 \implies a^{2n+1} < 0, \forall\ n \in \mathbb{N}$

Solução

c) $n = 0 \Rightarrow a^{2n+1} = a^1 = a < 0$, por hipótese. Suponhamos $a^{2r+1} < 0$, onde $r \geqslant 0$. Então: $a^{2(r+1)+1} = a^{2r+1} \cdot a^2 < 0$ pois $a^2 > 0$ e $a^{2r+1} < 0$ pela hipótese de indução.

3. Seja A um anel ordenado. Mostre que:

a) $(\forall\, a, b \in A)(a < b \implies a^3 < b^3)$

b) $(\forall\, a, b \in A)(a^5 = b^5 \implies a = b)$

4. Suponhamos que seja possível ordenar um anel de integridade de duas maneiras (não necessariamente distintas) e que P_1 e P_2 sejam os elementos positivos de cada uma dessas relações de ordem. Mostre que se $P_1 \subset P_2$, então $P_1 = P_2$.

5. Seja A um anel de integridade ordenável e L um subanel unitário de A. Mostre que L é ordenável.

Solução

Seja P o conjunto dos elementos positivos de A e consideremos $P' = P \cap L$. Mostremos que P' satisfaz, em relação a L, as condições da proposição 5. (i) $x, y \in P' \Rightarrow x, y \in P$ e $x, y \in L$. Logo $x + y \in P$ e $x + y \in L$. Assim $x + y \in P'$. (ii) análoga (iii) Seja $x \in L$. Então $x \in A$ e portanto $x \in P$ ou $x \in (-P)$. Se $x \in P$, então $x \in P' = P \cap L$. Se $x \in (-P)$, então $-x \in P$; mas de $x \in L$ decorre $-x \in L$ e portanto $(-x) \in P \cap L = P'$. (iv) Se $x \in P' \cap (-P')$, então $x \in P'$ e $x \in (-P')$. Daí $x \in P$ e $(-x) \in P$. Donde $x \in P \cap (-P) = \{0\}$.

6. Seja $\varphi : \mathbb{R} \longrightarrow \mathbb{R}$ um isomorfismo de anéis tal que $\varphi(\mathbb{R}_+) \subset \mathbb{R}_+$. Mostre que $a < b \implies \varphi(a) < \varphi(b)$, $\forall\ a, b \in \mathbb{R}$.

Solução

Como $a < b$, então $b - a > 0$. Daí $\varphi(b - a) \geqslant 0$ por hipótese. Se $\varphi(b - a) = 0$, como é injetora, então $b - a = 0$ o que é impossível. Donde $\varphi(b - a) = \varphi(b) - \varphi(a) > 0$ do que segue $\varphi(a) > \varphi(b)$.

7. Seja K um corpo ordenado. Mostre que $(1_K + na) \leqslant (1_K + a)^n$, $\forall\ n \in \mathbb{N}$ e para todo elemento positivo $a \in K$.

Solução

Se $n = 0$, então $1 + na = 1$ e $(1 + a)^n = (1 + a)^0 = 1$. Logo vale a igualdade neste caso. Suponhamos $(1 + ra) \leqslant (1 + a)^r$, onde $r \geqslant 0$. Daí, como $1 + a > 0$, segue que $(1 + ra)(1 + a) \leqslant (1 + a)^r (1 + a) = (1 + a)^{r+1}$. Como $0 \leqslant ra^2$, então $1 + (r + 1)a \leqslant 1 + (r + 1)a + ra^2 = (1 + ra)(1 + a)$. Donde $1 + (r + 1)a \leqslant (1 + a)^{r+1}$.

8. Seja K um corpo arquimediano (mesma definição de anel arquimediano). Se $a \in K$ e $1_K < a$, mostre que

a) $\forall\ b \in K \implies \exists\ n \in \mathbb{N} \mid b < a^n$

b) Se $b \in K$ e b é positivo, então $\exists\ n \in \mathbb{N}$ tal que $a^{-n} < b$

9. Mostre que um anel de integridade ordenado A não possui mínimo.

Solução

Para todo $m \in A$, $m - 1 \in A$ e $m - 1 < m$.

10. Seja K um corpo ordenado. Mostre que $a, b, c, d \in K$, se $b \neq 0$ e $d \neq 0$, então $a \cdot b^{-1} \leqslant c \cdot d^{-1} \iff a \cdot b \cdot d^2 \leqslant b^2 \cdot c \cdot d$.

Capítulo VI

ANÉIS FATORIAIS

§ 1º — DIVISIBILIDADE NUM ANEL DE INTEGRIDADE

1. ELEMENTOS ASSOCIADOS

Neste capítulo somente consideraremos anéis de integridade.

Seja A um tal anel. Dados $a, b \in A$, dizemos que a *divide* b ou que b é *divisível* por a se existe $c \in A$ de modo que $b = ac$. Se $a \neq 0$, o elemento c que figura nessa igualdade é chamado *quociente* de b por a e costuma ser indicado por $\frac{b}{a}$. Para indicar que a divide b usa-se a seguinte notação: $a \mid b$. Se a não divide b a notação para tal fato é $a \nmid b$.

Dessa forma ficou definida uma relação sobre o conjunto A para a qual são verdadeiras as seguintes propriedades:

a) Reflexiva

b) Transitiva

c) $(\forall\ a, b, c \in A)(a \mid b \implies a \mid bc)$

d) $(\forall\ a, b, c, x, y \in A)(a \mid b \text{ e } a \mid c \implies a \mid (bx + cy)$

Deixamos a cargo do leitor a demonstração dessas propriedades.

Definição 1: Dois elementos a e b de um anel de integridade se dizem *associados* se $a \mid b$ e $b \mid a$. Notação: $a \sim b$.

Exemplo: No anel $\mathbb{R}[X]$ os polinômios $f = 1 + X$ e $g = 2 + 2X$ são associados porque $2 + 2X = 2(1 + X)$ e $(1 + X) = \frac{1}{2}(2 + 2X)$.

Exercício: A relação $\sim$ definida acima sobre um anel de integridade é uma relação de equivalência.

Proposição 1: Sejam a e b elementos de um anel de integridade A. Então são equivalentes as seguintes afirmações: (i) $a \sim b$ (ii) $<a> = <b>$ (iii) $\exists\, u \in U(A)$ de maneira que $b = au$.

Demonstração:

(i) $\Longrightarrow$ (ii)

$a \sim b \Longrightarrow a \mid b$ e $b \mid a$. Logo existem $c_1, c_2 \in A$ de maneira que $b = ac_1$ e $a = bc_2$.

Seja $x \in <a>$. Então existe $t \in A$ de modo que $x = at$. Levando em conta que $a = bc_2$, temos $x = b(c_2 t)$, isto é, $x \in <b>$. Provamos assim que $<a> \subset <b>$. De modo análogo se prova que $<b> \subset <a>$.

(ii) $\Longrightarrow$ (iii)

Como $<a> = <b>$, então existe $t_1 \in A$ de maneira que $a = bt_1$. Analogamente, existe $t_2 \in A$ de modo que $b = at_2$, portanto, $a = a(t_2 t_1)$. Se $a = 0$, então $b = 0$ e, por exemplo, $0 = 0 \cdot 1$. Caso contrário a pode ser cancelado da igualdade $a = a(t_2 t_1)$ e chegamos à conclusão que $t_1 t_2 = 1$, isto é, t_1 e t_2 são inversíveis. Fazendo $t_2 = u$, então $b = au$, onde u é inversível em A.

(iii) $\Longrightarrow$ (i)

Da hipótese $b = au$ segue direto que $a \mid b$. Por outro lado, como u é inversível, $b = au \Longrightarrow a = bu^{-1}$. Donde $b \mid a$. ■

2. ELEMENTOS PRIMOS E IRREDUTÍVEIS

Definição 2: Um elemento $p \neq 0$ de um anel de integridade A se diz *primo* se $p \notin U(A)$ e se é verdadeiro o seguinte:

$$(\forall\, a, b \in A)(p \mid ab \Longrightarrow p \mid a \text{ ou } p \mid b).$$

Nota: Se p é primo no anel de integridade A, por indução pode-se provar que: $p \mid a_1 a_2 \ldots a_n \Longrightarrow \exists\, r,\ 1 \leqslant r \leqslant n$, de modo que $p \mid a_r$ $(n \geqslant 2)$.

Exemplo: Em $\mathbb{Z}[X]$ o elemento X é primo pois $X \neq 0$, X não é inversível e, além disso, supondo que $X \mid fg$, onde $f = a_0 + a_1 X + \ldots$ e $g = b_0 + b_1 X + \ldots$ então existem $c_0, c_1, \ldots \in \mathbb{Z}$ de maneira que

$$fg = a_0 b_0 + (a_0 b_1 + b_0 a_1)X + \ldots = c_0 X + c_1 X^2 + \ldots$$

Donde $a_0 b_0 = 0$. Daí $a_0 = 0$ ou $b_0 = 0$, ou seja, $X \mid f$ ou $X \mid g$.

Definição 3: Um elemento $p \neq 0$ de um anel de integridade A é chamado *irredutível* se $p \notin U(A)$ e se vale a seguinte frase:

$$(\forall\, a, b \in A)(p = ab \Longrightarrow a \in U(A) \text{ ou } b \in U(A)).$$

Um elemento $a \in A$, não nulo, não inversível e não irredutível chama-se *redutível* ou *composto*.

Exemplo: $X \in \mathbb{R}[X]$ é irredutível. É claro que X não é nulo e também não é inversível. Suponhamos $X = fg$. Como o grau de X é 1, então ou f ou g tem que ter grau 0. Ora, qualquer polinômio de grau zero em $\mathbb{R}[X]$ é inversível (e vice-versa).

Proposição 2: Todo elemento primo de um anel de integridade A é irredutível.

Demonstração: Seja $p \in A$ um elemento primo. Então $p \neq 0$ e $p \notin U(A)$. Suponhamos $p = ab$. Como $p \mid p$, então $p \mid ab$. Daí $p \mid a$ ou $p \mid b$.

Suponhamos $p \mid a$. Então existe $t \in A$ de modo que $a = pt$. Substituindo em $p = ab$ obtemos $p = p(tb)$. Donde $tb = 1$ o que mostra que b é inversível.

É claro que supondo $p \mid b$, teremos como conclusão que a é inversível. ■

Nota: A recíproca desta proposição não é verdadeira (ver exercício 16).

3. MÁXIMO DIVISOR COMUM

Definição 4: Seja A um anel de integridade. Dizemos que um elemento $d \in A$ é *máximo divisor comum* dos elementos $a, b \in A$ se

(i) $d \mid a$ e $d \mid b$; (ii) Se $d' \in A$, $d' \mid a$ e $d' \mid b$, então $d' \mid d$.

A definição de máximo divisor comum de n elementos $(n \geqslant 2)$ de um anel de integridade A é óbvia.

Dois elementos a e b de um anel de integridade A se dizem *primos entre si* se admitem a unidade de A como máximo divisor comum.

Proposição 3: Sejam a e b elementos de um anel de integridade A. Se d é máximo divisor comum de a e b e se $d_1 \sim d$, então d_1 também é máximo divisor comum de a e b. Reciprocamente, se d e d_1 são máximos divisores comuns de a e b, então $d \sim d_1$.

Demonstração:

- $d_1 \mid d$, $d \mid a$ e $d \mid b \Longrightarrow d_1 \mid a$ e $d_1 \mid b$.
  Se $d' \mid a$ e $d' \mid b$, então $d' \mid d$. Mas $d \mid d_1$. Logo $d' \mid d_1$.
- Se d e d_1 são máximos divisores comuns de a e b, então $d \mid d_1$ e $d_1 \mid d$. Logo $d \sim d_1$.

Nota: É claro então que dois elementos a e b de A são primos entre si se, e somente se, U(A) é o conjunto dos seus máximos divisores comuns.

4. ANÉIS QUADRÁTICOS

Seja $n \neq 1$ um número inteiro *livre de quadrados*. Isto é, um número inteiro cujo único divisor quadrado perfeito em $\mathbb{Z}$ é 1. Indiquemos por $\mathbb{Z}[\sqrt{n}]$ o seguinte subconjunto de $\mathbb{C}$:

$$\mathbb{Z}[\sqrt{n}] = \{x + y\sqrt{n} \mid x, y \in \mathbb{Z}\}$$

Para cada n, nas condições exigidas acima, o conjunto $\mathbb{Z}[\sqrt{n}]$ é subanel unitário de $\mathbb{C}$, o que se pode verificar de modo rotineiro. Logo cada um deles é um anel de integridade. Os $\mathbb{Z}[\sqrt{n}]$ assim obtidos são chamados *anéis quadráticos*. O anel quadrático em que $n = -1$ é chamado *anel dos inteiros de Gauss*.

Dado um elemento genérico $\alpha = a + b\sqrt{n}$ do anel quadrático $\mathbb{Z}[\sqrt{n}]$ define-se a *norma* de α (notação: $N(\alpha)$) do seguinte modo:

$$N(\alpha) = a^2 - b^2 n$$

Valem então as seguintes propriedades:

(i) $N(\alpha) = 0 \iff \alpha = 0$

(ii) $N(\alpha\beta) = N(\alpha)N(\beta)$, $\forall\ \alpha, \beta \in \mathbb{Z}[\sqrt{n}]$

(iii) $N(1) = 1$

(iv) $N(\alpha) = \pm 1 \iff \alpha$ é inversível em $\mathbb{Z}[\sqrt{n}]$.

(v) Se $N(\alpha)$ é um número primo p, então α é irredutível em $\mathbb{Z}[\sqrt{n}]$.

Provaremos as duas últimas.

(iv)

$(\Longrightarrow)$ $N(\alpha) = a^2 - b^2 n = 1 \Longrightarrow (a + b\sqrt{n})(a - b\sqrt{n}) = 1 \Longrightarrow \alpha \mid 1$

$(\Longleftarrow)$ $\alpha \mid 1 \Longrightarrow 1 = \alpha\beta\ (\beta \in \mathbb{Z}[\sqrt{n}]) \Longrightarrow 1 = N(\alpha)N(\beta) \Longrightarrow N(\alpha) \mid 1$ (em $\mathbb{Z}$) $\Longrightarrow N(\alpha) = \pm 1$.

(v)

Como $N(\alpha) \neq 1$ e $N(\alpha) \neq 0$, então $\alpha \neq 0$ e α não é inversível. Suponhamos $\alpha = \beta\gamma$, com β e $\gamma \in \mathbb{Z}[\sqrt{n}]$. Daí $p = N(\beta)N(\gamma)$. Logo $N(\beta) = \pm 1$ ou $N(\gamma) = \pm 1$. Ou seja: ou β ou γ é inversível. ■

EXERCÍCIOS

1. Mostre que a relação $x \mid y$ num anel de integridade não é nem simétrica nem antissimétrica, em geral.

2. Seja A um anel de integridade. Mostre que a relação R sobre A dada por $xRy \iff x \sim y$ (x associado de y) é uma relação de equivalência em A.

Determinar $A/\sim$ nos seguintes casos:

a) A é um corpo

b) $A = \mathbb{Z}$

c) $A = K[X]$, onde K é um corpo.

Seja A um anel de integridade e considere $a, u \in A$, onde u é inversível. Mostre que

a) a é irredutível $\iff$ au é irredutível

b) a é primo $\iff$ au é primo.

Sejam a e b elementos de um anel de integridade A. Mostre que

$\langle a \rangle \subset \langle b \rangle \iff b \mid a$

Sejam a e b dois elementos de um anel de integridade A que admitem um máximo divisor comum d nesse anel. Sendo $u \in U(A)$, mostre que d também é máximo divisor comum de au e b e de a e ub.

Mostre que o número 2 é respectivamente irredutível, redutível e inversível nos seguintes anéis

$$\mathbb{Z}\ ;\ \mathbb{Z}[i]\ \text{e}\ \mathbb{Q}$$

Solução

Em $\mathbb{Z}$, 2 é primo portanto 2 é irredutível.

Em $\mathbb{Z}[i]$, $N(2) = 4$. Se $\alpha\beta = 2$, então $N(\alpha) \cdot N(\beta) = 4$ e uma possibilidade é $N(\alpha) = N(\beta) = 2$ e $\alpha = 1 + i$ e $\beta = 1 - i$, portanto, $2 = (1 + i)(1 - i)$.

Em $\mathbb{Q}$, $2 \cdot \frac{1}{2} = 1$ e $2 \in U(\mathbb{Q})$.

Determinar todos os elementos inversíveis dos seguintes anéis quadráticos

$$\mathbb{Z}[i] \quad \text{e} \quad \mathbb{Z}[\sqrt{-5}]$$

Siga o roteiro abaixo para mostrar que existem infinitos elementos inversíveis no anel $A = \mathbb{Z}[\sqrt{2}]$.

a) Determine um elemento $\alpha \in A$, $\alpha \neq \pm 1$, que seja inversível;

b) Mostre que se α é inversível, então α^n é inversível, $\forall\ n \geqslant 1$ $(n \in \mathbb{N})$;

c) Considere a seguinte seqüência de elementos de A: $1, \alpha, \alpha^2, \ldots$.

Mostre que $1 + 2\sqrt{2}$ é irredutível em $\mathbb{Z}[\sqrt{2}]$. Mesmo exercício com $\sqrt{2}$.

Mostre que o polinômio $f = 2 + 2X + 4X^2$ é irredutível como elemento de $\mathbb{R}[X]$ mas é redutível em $\mathbb{Z}[X]$.

Sejam a e b elementos associados de um anel de integridade A. Se $c \in A$, mostre que

a) $c \mid a \iff c \mid b$;

b) $a \mid c \iff b \mid c$;

c) $b \sim c \iff xb \sim xc, \forall\ x \in A^*$

13. Mostre que são irredutíveis no anel dos inteiros de Gauss:
$1+i$, $1-i$ e 3

14. Determine todos os divisores do número $2 \in \mathbb{Z}[i]$.

Sugestão: $\alpha \mid 2 \Rightarrow 2 = \alpha \cdot \beta \Rightarrow 4 = N(\alpha) \cdot N(\beta) \Rightarrow N(\alpha) \mid 4$ (em $\mathbb{Z}$).

Com isto acham-se todos os divisores de 2 e, eventualmente, outros elementos. Daí é só testar.

15. Determine um máximo divisor comum de $1+i$ e $1-i$, no anel $A = \mathbb{Z}[i]$.

16. Mostre que o número 3 é irredutível no anel $A = \mathbb{Z}[\sqrt{-5}]$ mas não é primo neste anel.

Sugestão: Para a segunda parte mostre que $3 \mid (2 + i\sqrt{5})(2 - i\sqrt{5})$ mas que não divide nenhum desses fatores.

17. Mostre que no anel do exercício anterior os elementos 9 e $6 + 3\sqrt{-5}$ não admitem máximo divisor comum.

Sugestão: Ache os divisores de cada um deles (conforme exercício 14) e verifique que nenhum divisor comum é máximo divisor comum (não satisfazem a segunda parte da definição de m . d . c .).

18. Seja p um número inteiro primo. Mostre que p é irredutível como elemento de $\mathbb{Z}[i]$ se, e somente se, a equação $x^2 + y^2 = p$ não admite soluções inteiras (soluções em $\mathbb{Z}$).

19. Prove que todo número primo $p = 4n+3$ ($n \in \mathbb{Z}$) é irredutível em $\mathbb{Z}[i]$.

Sugestão: Use o exercício anterior.

§ 2º — ANÉIS PRINCIPAIS — ANÉIS FATORIAIS

1. ANÉIS PRINCIPAIS

Já definimos anteriormente o que vem a ser um anel principal: é um anel de integridade cujos ideais são todos principais. São exemplos importantes de anéis principais, conforme já vimos, o anel $\mathbb{Z}$ dos inteiros e os anéis $K[X]$, onde K é um corpo.

Mostraremos neste item algumas propriedades importantes relacionadas com a divisibilidade nesses anéis.

Proposição 4: Num anel principal todo elemento irredutível é primo.

Demonstração: Seja p um elemento irredutível. Logo $p \neq 0$ e $p \notin U(A)$. Suponhamos que $p \mid ab$, onde $a, b \in A$. Mostremos que p divide um desses elementos.

Seja $< p, a > = < d >$. Como p pertence a esse ideal, existe $q \in A$ de maneira que $p = dq$. Sendo p irredutível, então ou d é inversível ou q é inversível.

Se $d \in U(A)$, então $< p, a > = A$. Logo existem $x, y \in A$ de maneira que $1 = px + ay$. Multiplicando por b esta igualdade obtemos: $b = p(bx) + (ab)y$. Como p divide ambas as parcelas do segundo membro desta relação, concluimos então que $p \mid b$.

Agora, se $q \in U(A)$, então de $p = dq$ segue que $d = pq^{-1}$. Como, por outro lado, $a \in < d >$, então $a = dq_1$, com $q_1 \in A$. Portanto $a = p(q^{-1}q_1)$, o que nos garante que $p \mid a$. ■

Proposição 5: Num anel principal A dois elementos quaisquer a e b admitem máximo divisor comum em A.

Demonstração: Consideremos o ideal $I = < a, b >$. Como A é principal existe então $d \in A$ de modo que $I = < d >$. Mostremos que d é máximo divisor comum de a e b.

- $a = a \cdot 1 + b \cdot 0 \Longrightarrow a \in I$. Logo existe $q \in A$ de modo que $a = dq$. Portanto $d \mid a$. Do mesmo modo se prova que $d \mid b$.
- Como $d \in I$, existem $x_0, y_0 \in A$ de maneira que $d = ax_0 + by_0$. Se d' é um elemento de A que divide a e b, esta última igualdade nos garante que $d' \mid d$. ■

Nota: Os elementos x_0 e y_0 da demonstração acima não são em geral únicos. Toda igualdade $d = ax_0 + by_0$, nas condições do teorema, chama-se *identidade de Bezout* para os elementos a e b.

Proposição 6: Um elemento $p \neq 0$ de um anel principal A é irredutível se, e somente se, o ideal $< p >$ é maximal.

Demonstração: ($\Longrightarrow$) Suponhamos p irredutível e admitamos que $< a >$ seja um ideal em A tal que $< p > \subsetneq < a >$. Então existe $q \in A$ de maneira que $p = aq$. Sendo p irredutível há duas alternativas: $q \in U(A)$ ou $a \in U(A)$.

A primeira deve ser descartada pois acarretaria $< p > = < a >$.

Então a é inversível, do que resulta $< a > = A$.

($\Longleftarrow$) Suponhamos $< p >$ maximal. Então $p \notin U(A)$ (pois $p \in U(A) \Longrightarrow$ $\Longrightarrow < p > = A$). Se $p = ab$, então $< p > \subset < a >$. Donde $< a > = < p >$ ou $< a > = A$. O primeiro caso leva a $a \sim p$ e portanto a que $b \in U(A)$. O segundo caso nos conduz a que $a \in U(A)$. ■

Nosso objetivo a seguir é provar que todo elemento não nulo e não inversível de um anel principal pode ser fatorado em elementos irredutíveis, num certo sentido de "maneira única". Os lemas a seguir visam a chegar a esse ponto.

Lema 1: Seja $I_1 \subset I_2 \subset I_3 \subset \ldots$ uma seqüência de ideais num anel principal A. Então existe $r \geqslant 1$ de modo que $I_r = I_{r+1} = \ldots$

Demonstração:

Seja $I = \bigcup_{n=1}^{\infty} I_n$. O conjunto I é um ideal em A (ver exercício 79-cap. 3). Logo existe $d \in A$ tal que $I = < d >$. Estando d em I, existe $r \geqslant 1$ de maneira que $d \in I_r$. Mostremos que $I = I_r$. Para tanto basta provar que $I \subset I_r$.

Se $x \in I$, existe $q \in A$ tal que $x = dq$. Como $d \in I_r$, x também pertence a I_r. Assim efetivamente $I \subset I_r$.

É evidente então que $I_r = I_{r+1} = \ldots$

Lema 2: Seja A um anel principal. Então um elemento $a \in A$, não nulo e não inversível, admite um divisor irredutível.

Demonstração: Formemos o ideal $I_0 = < a >$. Se este ideal é maximal então a é irredutível.

Caso contrário, existe $a_1 \in A$ de maneira que $I_0 \subsetneq I_1 = < a_1 >$. Se o ideal I_1 é maximal, temos que a_1 é irredutível.

Caso contrário, existe $a_2 \in A$ de tal modo que $I_0 \subsetneq I_1 \subsetneq I_2 = < a_2 >$.

Como a seqüência de ideais assim obtida é estacionária (lema 1), existirá então um índice $r \geqslant 0$ de tal modo que I_r é maximal. O gerador a_r deste ideal ($a_r = a$, se $r = 0$) é irredutível e $a_r \mid a$ pois $< a > \subset < a_r >$. ■

Teorema 1 *(Fatoração "única")*: Seja A um anel principal. Dado um elemento $a \in A$, não nulo e não inversível, existem elementos irredutíveis $p_1, p_2, \ldots, p_n$ ($n \geqslant 1$) de maneira que $a = p_1 p_2 \ldots p_n$. Além disso, se $a = q_1 q_2 \ldots q_s$, com os q_j irredutíveis, então $n = s$ e cada fator p_i da primeira decomposição é associado de um fator q_j da segunda decomposição.

Demonstração:

(Existência) É trivial o caso em que a é irredutível. Suponhamos a um elemento composto de A. Então existe um elemento irredutível $p_1 \in A$ tal que $a = p_1 q_1$ ($q_1 \in A$). Devido à hipótese feita por último, podemos dizer que $q_1 \notin U(A)$. Caso q_1 seja irredutível o teorema está provado nesta parte (com $n = 2$). Se não, existe um elemento irredutível p_2 que divide q_1: $q_1 = p_2 q_2$ ($q_2 \in A$). Então $a = p_1 p_2 q_2$, onde q_2 não é inversível. Nessa seqüência de idéias existirá um $n > 1$ de maneira que q_{n-1} é irredutível (por quê?). Fazendo $q_{n-1} = p_n$ obtemos a decomposição desejada

$$a = p_1 p_2 \ldots p_n$$

("Unicidade") Suponhamos $a = p_1 p_2 \ldots p_n = q_1 q_2 \ldots q_s$. Como $p_1 \mid a$, então $p_1 \mid q_1 q_2 \ldots q_s$. Sendo p_1 um elemento primo, p_1 divide um dos q_j. Admitamos que $p_1 \mid q_1$. Como q_1 também é primo segue disso que $p_1 \sim q_1$.

Suponhamos $q_1 = u_1 p_1$ (com $u_1 \in U(A)$). Então de $p_1 p_2 \ldots p_n = q_1 q_2 \ldots q_s$ tiramos que $p_2 p_3 \ldots p_n = (u_1 q_2) q_3 \ldots q_s$. Usando a mesma argumentação desenvolvida até aqui, só que com relação a esta última igualdade, chegaremos a algo assim: $p_2 \sim q_2$.

A repetição desse raciocínio nos levará à "unicidade" nos termos enunciados. ■

2. ANÉIS FATORIAIS

Introduziremos agora uma categoria de anéis mais geral que a dos anéis principais em que nos detivemos até agora. O teorema anterior serve de motivação para a definição a ser dada agora.

Definição 5: Um anel de integridade A recebe o nome de *anel fatorial* se (i) todo elemento $a \in A$, não nulo e não inversível, pode ser fatorado do seguinte modo: $a = p_1 p_2 \ldots p_n$, onde $n \geqslant 1$ e os p_i irredutíveis; (ii) se $a = q_1 q_2 \ldots q_s$, onde $s \geqslant 1$ e os q_j são também irredutíveis, então $n = s$ e cada fator p_i é associado de um fator q_j. Ou seja, vale o teorema da fatoração "única".

É claro, pelo que vimos, que os anéis principais são todos fatoriais. A recíproca desse fato, contudo, não é verdadeira conforme veremos ao fim deste capítulo.

Nota: Numa decomposição $a = p_1 p_2 \ldots p_n$, com os p_i irredutíveis, pode-se ter, para alguns pares de fatores, $i \neq j$ e $p_i \sim p_j$. Contudo é conveniente "reunir" os fatores associados entre si. Dessa maneira a decomposição assume o seguinte aspecto:

$$a = u p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$$

na qual u é inversível, $1 \leqslant r \leqslant n$, cada $\alpha_i \geqslant 1$ e $p_i \not\sim p_j$ sempre que $i \neq j$.

Às vezes, quando se têm dois ou mais elementos na mesma questão, todos não nulos e não inversíveis, convém (e é possível) escrever a decomposição de cada um deles em fatores irredutíveis de maneira que esses fatores sejam exatamente os mesmos em todas as decomposições. Para tanto, supondo que um fator irredutível p figura explicitamente em $a \in A$ e não figura explicitamente em $b \in A$, colocamos p como fator de b com expoente zero. Assim, supondo que sejam dois os elementos, a e b, será possível o seguinte:

$$a = u p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n} \quad \text{e} \quad b = v p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n}$$

onde u e v são inversíveis, $n \geqslant 1$, $\alpha_i, \beta_i \geqslant 0$ $(i = 1, \ldots, n)$ e $p_i \not\sim p_j$ sempre que $i \neq j$.

Por exemplo, no anel $\mathbb{R}[X]$ os polinômios $f = 1 - X^2$ e $g = 1 - 2X + X^2$ podem ser representados assim:

$$f = (1 - X)(1 + X) \quad \text{e} \quad g = (1 - X)^2 (1 + X)^0$$

Proposição 7: Num anel fatorial A todo elemento irredutível $p \in A$ é primo.

Demonstração: Suponhamos que $a, b \in A$ e que $p \mid ab$. Se $a \in U(A)$, então $p \mid b$. Do mesmo modo, se $b \in U(A)$, é claro que $p \mid a$. Também são triviais os casos em que $a = 0$ ou $b = 0$.

Suponhamos a e b não nulos e não inversíveis. Como $p \mid ab$, por hipótese, então existe $c \in A$ tal que $ab = pc$. Sejam

$$a = p_1 p_2 \ldots p_m \quad \text{e} \quad b = q_1 q_2 \ldots q_n$$

"as" decomposições de a e b em fatores irredutíveis. Então

$$p_1 \ldots p_m q_1 \ldots q_n = pc$$

Pela definição de anel fatorial (parte (ii)) p deve ser associado ou de um dos p_i ou de um dos q_j. No primeiro caso $p \mid a$ e, se acontecer o segundo, $p \mid b$. ■

Proposição 8: Seja A um anel fatorial. Dados $a, b \in A$, existe máximo divisor comum desses elementos em A.

Demonstração: Se $a = 0$ $(b = 0)$, então b (respectivamente a) é um máximo divisor comum de a e b. Se $a \in U(A)$ $(b \in U(A))$, então a (respectivamente b) é um máximo divisor comum de a e b (verifique).

Caso contrário decomponhamos a e b segundo observação final contida na nota anterior:

$$a = u p_1^{r_1} p_2^{r_2} \ldots p_n^{r_n} \quad \text{e} \quad b = v p_1^{s_1} p_2^{s_2} \ldots p_n^{s_n}$$

Mostremos que o elemento $d = p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}$, onde $k_i = \min \{r_i, s_i\}$ $(i = 1, \ldots, n)$ é um máximo divisor comum de a e b.

Que d divide a e divide b é imediato.

Suponhamos que $d' \in A$, $d' \mid a$ e $d' \mid b$. Então $d' = w p_1^{t_1} p_2^{t_2} \ldots p_n^{t_n}$ $(w \in U(A))$ e $t_i \leqslant r_i, s_i$. Logo $t_i \leqslant \min \{r_i, s_i\}$ $(i = 1, 2, \ldots, n)$. Donde $d' \mid d$. ■

Corolário 1: Se $d \neq 0$ é um máximo divisor comum de a e b, então $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si.

Demonstração: Mantendo as notações da proposição temos

$$\frac{a}{d} = u p_1^{r_1 - k_1} p_2^{r_2 - k_2} \ldots p_n^{r_n - k_n} \quad \text{e} \quad \frac{b}{d} = v p_1^{s_1 - k_1} p_2^{s_2 - k_2} \ldots p_n^{s_n - k_n}$$

Ora, como $k_i = \min \{r_i, s_i\}$, então quando não se tem $r_i - k_i = 0$ tem-se $s_i - k_i = 0$. Pela proposição $p_1^0 p_2^0 \ldots p_n^0 = 1$ é máximo divisor comum de a e b. Ou seja, a e b são primos entre si. ■

Corolário 2: Sejam a, b e $d \neq 0$ elementos de um anel principal A. Se d é máximo divisor comum de a e b, então $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si.

Demonstração: É só lembrar que os anéis principais são fatoriais. ■

3. ANÉIS EUCLIDIANOS

Vamos introduzir agora uma categoria especial de anéis principais.

Definição 6: Um anel de integridade A recebe o nome de *anel euclidiano* se existe uma função $d: A^* \longrightarrow \mathbb{N}$ com as seguintes propriedades:

(a) $d(ab) \geqslant d(a)$, $\forall\, a, b \in A^*$;

(b) $\forall$ $a, b \in A$, se $b \neq 0$, então existem $q, r \in A$ de maneira que $a = bq + r$, onde $r = 0$ ou $d(r) < d(b)$.

Os elementos q e r são chamados, respectivamente, quociente e resto, na divisão euclidiana (segundo a função d) de a por b.

Logo um anel euclidiano é um anel de integridade no qual existe uma divisão com resto.

Exemplos:

1) Sendo K um corpo, o anel K[X] é um anel euclidiano em relação à função "grau". Verifique.

2) O anel $\mathbb{Q}$ dos racionais é euclidiano em relação à função $d : \mathbb{Q}^* \longrightarrow \mathbb{N}$ dada por $d(r) = 1$, $\forall\ r \in \mathbb{Q}^*$, o que é bastante simples de verificar.

3) O anel $\mathbb{Z}[i]$ dos inteiros de Gauss é euclidiano em relação à função que associa a cada $\alpha \in \mathbb{Z}[i]$ a sua norma. Provemos este fato.

Lembremos que se $\alpha = a + bi \in \mathbb{Z}[i]$, sua norma é dada por $N(\alpha) = a^2 + b^2$.

Dados α e $\beta \in A$, com $\beta \neq 0$, então $\alpha\beta^{-1} = r + si$, onde $r, s \in \mathbb{Q}$. Tomemos $m, n \in \mathbb{Z}$ de maneira que

$$|r - m| \leqslant \frac{1}{2} \qquad \text{e} \qquad |s - n| \leqslant \frac{1}{2}$$

o que sempre é possível. Podemos escrever então

$$\alpha\beta^{-1} = m + ni + (r - m) + (s - n)i$$

Fazendo $m + ni = \gamma$ e $\beta[(r - m) + (s - n)i] = \delta$, ficamos com

$$\alpha = \beta\gamma + \delta$$

onde, caso $\delta \neq 0$,

$$d(\delta) = d(\beta)[(r - m)^2 + (s - n)^2] < d(\beta).$$

Isso mostra que γ e δ são, respectivamente, quociente e resto, na divisão de α por β, segundo a definição dada.

Proposição 9: Todo anel euclidiano é principal.

Demonstração: Seja A um anel euclidiano e tomemos um ideal I em A de modo que $I \neq <0>$. Tomemos em I um elemento b tal que

$$d(b) = \min \{d(x) \mid x \in I - \{0\}\}.$$

Raciocinando como já o fizemos para K[X] (onde K é um corpo) no capítulo anterior, chegaremos a que $I = <b>$. ■

EXERCÍCIOS

20. Decompor em fatores irredutíveis os seguintes inteiros de Gauss:
5, 3 + i, 4, 2i e 11

21. *Ache todos os máximos divisores comuns de* $3 + 6i$ *e* $2i$ *no anel* $\mathbb{Z}[i]$.
Mesmo exercício com 4 e 1 + i.

22. Sejam I, J e K ideais de um anel principal A. Prove que
(a) $I + (J \cap K) = (I + J) \cap (I + K)$
(b) $I \cap (J + K) = (I \cap J) + (I \cap K)$

24. Sejam a, b e c elementos não nulos de um anel principal. Prove que:
a) mdc (a, 1) ~ 1
b) mdc (ca, cb) ~ c · mdc (a, b)
c) mdc (a, b) ~ 1 e mdc (a, c) ~ 1 $\Longrightarrow$ mdc (a, bc) ~ 1
d) mdc (a, b) ~ 1, $a \mid c$ e $b \mid c \Longrightarrow ab \mid c$

Observação: mdc(x, y) indica aqui um máximo divisor comum qualquer de $x, y \in A$.

25. Mostre que $\mathbb{Z}[\sqrt{-5}]$ não é principal.
Sugestão: Mostre que o ideal $(3, 2 + \sqrt{-5})$ não é principal.

26. Mostre que $\mathbb{Z}[X]$ não é principal.
Sugestão: Considere o ideal, $<X, 2>$.

27. Mostre que $\mathbb{Z}[\sqrt{-6}]$ não é fatorial.
Sugestão: Mostre que $10 \in \mathbb{Z}[\sqrt{-6}]$ não obedece ao teorema da fatoração única.

28. *Mesmo exercício com* $A = \mathbb{Z}[\sqrt{-7}]$.
Sugestão: Considere $B \in \mathbb{Z}[\sqrt{-7}]$.

29. Seja A um anel euclidiano. Dado $a \in A^*$, mostre que
a) $d(a) \geqslant d(1)$
b) $d(a) = d(1) \Longleftrightarrow a \in U(A)$

30. Mostre que são euclidianos os seguintes anéis: $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{-2}]$ e $\mathbb{Z}[\sqrt{3}]$.
Sugestão: $d : (\mathbb{Z}[\sqrt{n}])^* \longrightarrow \mathbb{N}$ é neste caso definida por $d(\alpha) = |N(\alpha)|$, $\forall\ \alpha$. Proceda então como foi feito no anel dos inteiros de Gauss.

31. Seja I um ideal em $\mathbb{Z}[i]$. Mostre que $\mathbb{Z}[i] / I$ é finito.
Sugestão: Observar que $I = <\alpha>$. Use então o algoritmo da divisão e divida por α um elemento β qualquer de $\mathbb{Z}[i]$.

32. Num anel de integridade A define-se *mínimo múltiplo comum* de $a, b \in A$ como sendo um elemento $m \in A$ tal que: (i) $a \mid m$; $b \mid m$; (ii) $a \mid m'$ e $b \mid m' \Rightarrow m \mid m'$.
(I) Mostre, que num anel principal, qualquer gerador de $<a> \cap <b>$ é mínimo múltiplo comum de a e b.
(II) Mostre que, ainda num anel principal, $ab \sim md$, onde m é mínimo múltiplo comum e d é máximo divisor comum de a e b.

33. Se o anel de integridade A não é corpo, prove que A[X] não é euclidiano em relação à função ∂ (grau).

§ 3º — POLINÔMIOS SOBRE UM ANEL FATORIAL

Os anéis que intervirão neste parágrafo são todos fatoriais.

Definição 7: Seja A um anel fatorial. Dizemos que um polinômio $f = a_0 + a_1X + \ldots + a_nX^n \in A[X]$ é *primitivo* se f não é constante e se os seus coeficientes são primos entre si, isto é, admitem a unidade de A como máximo divisor comum.

Nota: Como A é fatorial, levando em conta a proposição 8 deste capítulo e raciocinando sobre ela por indução, podemos garantir que existe máximo divisor comum de $a_0, a_1, \ldots, a_n$ em A.

Exemplos

1) O polinômio $f = 2 + 2X + 3X^2 \in \mathbb{Z}[X]$ é primitivo.

2) $f = 2 + 2X + 4X^2$ é primitivo em $\mathbb{R}[X]$. Por que?

3) Se A é fatorial e $f \in A[X]$ é irredutível, então f é primitivo. De fato. Suponhamos f não primitivo. Então $f = df^*$, onde d é máximo divisor comum dos coeficientes de f e, portanto, $d \notin U(A) = U(A[X])$. Por outro lado f^* também não é inversível em A[X] já que $\partial(f) = \partial(f^*)$. Chegamos então à conclusão que f é composto. Absurdo.

4) Um polinômio primitivo pode ser redutível. Por exemplo $f = 2 + 5X + 2X^2 \in \mathbb{Z}[X]$ é primitivo em $\mathbb{Z}[X]$ e ao mesmo tampo composto pois

$$f = (2X + 1)(X + 2).$$

O resultado principal neste parágrafo é que "se um anel A é fatorial então A[X] também é fatorial". Alguns lemas serão necessários para chegarmos a esse resultado.

Lema 1: Seja $f \in A[X]$ um polinômio não constante. Então existe um polinômio primitivo $f^* \in A[X]$ e existe um elemento $d \in A$ de maneira que $f = df^*$. Além disso, se $f = d_1 f_1^*$, com $d_1 \in A$ e f_1^* primitivo em A[X], então $d \sim d_1$ e $f^* \sim f_1^*$.

Demonstração:

• Suponhamos $f = a_0 + a_1X + \ldots + a_nX^n$. Se d é um mdc de $a_0, a_1, \ldots, a_n$ fazendo

$$f^* = \frac{a_0}{d} + \frac{a_1}{d} X + \ldots + \frac{a_n}{d} X^n$$

temos evidentemente $f = df^*$ e, ainda, que f^* é primitivo, isto devido ao corolário 1, da proposição 8, deste capítulo.

• Suponhamos $f = df^* = d_1 f_1^*$. Da igualdade $f = d_1 f_1^*$ decorre que $d_1 \mid a_i$ $(i = 0, 1, \ldots, n)$. Logo $d_1 \mid d$. Donde, existe $c \in A$ de modo que $d = d_1 c$. Retomando a igualdade $df^* = d_1 f_1^*$ e levando em conta a última igualdade obtida chegamos a $d_1 cf^* = d_1 f_1^*$. Daí $cf^* = f_1^*$. Isto nos garante que c divide todos os coeficientes de f_1^*. Sendo este polinômio irredutível a conclusão é que c é inversível. Então $d \sim d_1$ e $f^* \sim f_1^*$. ■

Lema 2 (Gauss): O produto de dois polinômios primitivos sobre um anel fatorial é um polinômio primitivo.

Demonstração: Sejam $f = a_0 + a_1X + \ldots + a_mX^m$ e $g = b_0 + b_1X + \ldots + b_nX^n$ os polinômios primitivos, de graus m e n respectivamente. Então

$$fg = c_0 + c_1X + \ldots + c_{m+n}X^{m+n}$$

onde $c_k = \sum_{i+j=k} a_ib_j$ $(k = 0, 1, 2, \ldots)$

Se fg não fosse primitivo existiria um elemento irredutível $p \in A$ de modo que $p \mid c_k$ $(k = 0, 1, 2, \ldots, m+n)$. O elemento p dividindo $a_0 b_0$ e sendo irredutível, dividirá a_0 ou b_0.

Considerando a primeira alternativa, podemos dizer que $\exists\, r$, $0 < r \leqslant m$, de maneira que $p \mid a_0, p \mid a_1, \ldots, p \mid a_{r-1}$ e $p \nmid a_r$.

Como

$$c_r = a_0b_r + a_1b_{r-1} + \ldots + a_rb_0$$

$p \mid c_r$ e $p \nmid a_r$, então $p \mid b_0$.

Logo, podemos dizer que $\exists\, s$, $0 < s \leqslant n$, de sorte que $p \mid b_0$, $p \mid b_1, \ldots, p \mid b_{s-1}$ e $p \nmid b_s$. Levando em conta que

$$c_{r+s} = a_0b_{r+s} \ldots a_{r-1}b_{s+1} + a_rb_s + a_{r+1}b_{s-1} + \ldots + a_{r+s}b_0$$

então $p \mid a_rb_s$. Donde $p \mid a_r$ ou $p \mid b_s$. Absurdo. ■

Lema 3: Seja K o corpo das frações de um anel fatorial A. Se $F \in K[X]$ não é constante, então existem $a, b \in A^*$ e um polinômio primitivo $f^* \in A[X]$ de maneira que $F = \frac{a}{b} f^*$. Além disso, se $F = \frac{a_1}{b_1} f_1^*$, com $a_1, b_1 \in A^*$ e $f_1^* \in A[X]$ também primitivo, então $ab_1 \sim a_1b$ e $f^* \sim f_1^*$.

Demonstração:

Sendo $F = \frac{c_0}{d_0} + \frac{c_1}{d_1} X + \ldots + \frac{c_m}{d_m} X^m$ e fazendo $d_0d_1 \ldots d_m = b$, então $F = \frac{1}{b} f$, onde $f \in A[X]$. Usando o lema 1: $F = \frac{a}{b} f^*$, com f^* primitivo e $a \in A^*$.

Por outro lado, se $F = \frac{a}{b} f^* = \frac{a_1}{b_1} f_1^*$, conforme o enunciado, então $ab_1 f^* = a_1 b f_1^*$. Usando mais uma vez o lema 1 (sua segunda parte) podemos concluir que $ab_1 \sim a_1 b$ e que $f^* \sim f_1^*$. ■

Lema 4 (Gauss): Seja f um polinômio irredutível sobre o anel fatorial A. Se K indica o corpo das frações de A, então f também é irredutível sobre K.

Demonstração: Suponhamos f redutível sobre K. Então existem dois polinômios G, H $\in$ K[X], ambos de grau maior que ou igual a 1, tais que f = GH. O lema 3 nos permite o seguinte com relação a G e a H:

$G = \frac{a}{b} g$ e $H = \frac{c}{d} h$, onde a, b, c, d $\in A^*$ e g, h $\in$ A[X] são primitivos.

Assim temos

$$f = \frac{ac}{bd} gh \quad \text{ou} \quad bdf = ac(gh)$$

onde gh é primitivo, devido ao lema 2.

Então $\exists$ u $\in$ U(A) de forma que ac = u(bd)(pois ac e bd são associados) Portanto f = (ug)h. Como $\partial(ug) = \partial(G) \geqslant 1$ e $\partial(h) = \partial(H) \geqslant 1$, então a igualdade f = (ug)h nos diz que f é redutível em A[X], o que é contrário à hipótese. ■.

Nota: Da demonstração que acabamos de fazer decorre que se f $\in$ A[X] se decompõe em K[X] em dois fatores, G e H, ambos de grau $\geqslant 1$, então f também se decompõe em A[X] em dois fatores, g e h, de graus respectivamente iguais aos de G e de H.

Corolário: Seja A um anel fatorial. Então todo polinômio irredutível f $\in$ A[X] é também primo.

Demonstração: Suponhamos primeiro que f $\in$ A, isto é, que f é um polinômio constante. Sendo irredutível como elemento de A, então f é primo em A. Logo (ver exercício 36) f é primo em A[X].

Vamos supor agora que $\partial(f) \geqslant 1$ e admitir que f | gh em A[X]. Se K é o corpo das frações de A, podemos dizer então que f | gh em K[X]. Como K[X] é um anel principal e f é primo em K[X] (por quê?), então f | g ou f | h (em K[X]). Consideremos a primeira alternativa.

Dela tiramos que existe M $\in$ K[X] tal que g = fM. Usando as decomposições dadas pelos lemas 1 e 3 e lembrando que f é primitivo em A[X], pois é irredutível neste anel, obtemos

$$cg^* = \frac{a}{b} fm^*$$

onde a, b, c $\in A^*$ e g^* e fm^* são polinômios primitivos de A[X]. Então bc $\sim$ a o que acarreta que existe u $\in$ U(A) tal que

$$g^* = ufm^*.$$

Logo g = f(ucm*), o que garante que f | g em A[X]. ■

Teorema 2: Se A é um anel fatorial, então A[X] também é fatorial.

Demonstração: Seja f $\in$ A[X], f $\neq 0$ e f não inversível.

• (Decomposição). Procederemos por indução.

Se $\partial(f) = 0$, então f $\in$ A. Decompondo f em fatores irredutíveis de A (o que é possível pois A é fatorial) teremos a decomposição desejada, pois um elemento irredutível em A também o é em A[X] (justifique).

Suponhamos que o grau de f seja $n > 0$ e admitamos que a decomposição seja possível para todo polinômio de grau r, onde $0 \leqslant r < n$. Devido ao lema 1 podemos escrever $f = df^*$, onde d $\in$ A e $f^* \in$ A[X] é primitivo. Caso f^* seja irredutível, decompomos d em fatores irredutíveis em A obtendo a decomposição pretendida para f. (Neste caso, se d fosse inversível, então f também seria irredutível e nada haveria a fazer.) Caso f^* seja composto, existem então g, h $\in$ A[X] de modo que

$f^* = gh$, sendo que $1 \leqslant \partial(g), \partial(h) < \partial(f^*) = \partial(f)$.

Aplicando a hipótese de indução para g e para h e raciocinando com d como nos outros casos, a demonstração se completará.

• (Unicidade) Por indução. Fica como exercício. O leitor poderá inspirar-se, se for o caso, no que foi feito no teorema 1. E deverá notar que o último corolário é peça fundamental da demonstração a ser feita. ■

Nota: Em virtude do teorema demonstrado podemos afirmar que $\mathbb{Z}[X]$ é um anel fatorial (já que $\mathbb{Z}$ é fatorial). Contudo $\mathbb{Z}[X]$ não é um anel principal. Para garantir tal afirmação mostremos que o ideal $I = \langle 2, X \rangle$ não é principal. Se fosse existiria f $\in$ I de modo que $I = \langle f \rangle$. Como 2 e X pertencem a I poderiam ser assim representados: 2 = fg e X = fh, onde g e h são polinômios convenientes de $\mathbb{Z}[X]$. Da primeira dessas igualdades tiramos que $f = \pm 1$ ou $f = \pm 2$. Levando em conta também a segunda ficamos com $f = \pm 1$. Daí seria possível representar o número 1 da seguinte forma: $1 = 2m_1 + Xm_2$, com $m_1, m_2 \in Z[X]$, o que é absurdo.

Critério de Eisenstein: Seja A um anel fatorial e seja K o seu corpo de frações. Dado $f = a_0 + a_1 X + \ldots + a_n X^n \in A[X]$ (f não constante), se existir um elemento irredutível p $\in$ A tal que $p \mid a_0, p \mid a_1, \ldots, p \mid a_{n-1}, p \nmid a_n$ e $p^2 \nmid a_0$ então f é irredutível em K[X].

Demonstração: Seja $f = GH$ uma decomposição de f em $K[X]$. Vamos supor $\partial(F) = r$ e $\partial(G) = s$. Conforme nota logo após o lema 4, f se decompõe também em $A[X]$ em um par de fatores, de graus r e s. Seja

$$f = (b_0 + b_1 X + \ldots + b_r X^r)(c_0 + c_1 X + \ldots + c_s X^s)$$

essa decomposição. Como $p \mid b_0 c_0 = a_0$ e $p^2 \nmid a_0$, então $p \mid c_0$ ou $p \mid b_0$ ("ou" exclusivo). Suponhamos que $p \mid b_0$. Como $p \nmid b_r c_s = a_n$, então $p \nmid b_r$. Admitamos que $p \mid b_0, p \mid b_1, \ldots, p \mid b_{k-1}$ e $p \nmid b_k$, onde $0 < k \leqslant r \leqslant n$. Considerando o termo

$$a_k = b_0 c_k + \ldots + b_{k-1} c_1 + b_k c_0$$

concluímos então que $p \nmid a_k$ (se dividisse teria que dividir também b_k ou c_0). Donde $k = n$. Assim $r = n$ e, consequentemente, $s = 0$.

Provamos pois que uma decomposição qualquer de f em $K[X]$ em dois fatores só é possível se um desses fatores for de grau zero. Isto significa que f é irredutível em $K[X]$. ■

Exemplo: Consideremos o polinômio $f = 7 + 14X + X^6$ de $\mathbb{Z}[X]$. Tomando o número primo $p = 7$ verificamos que 7 divide todos os coeficientes de f exceto o do termo em X^6. Por outro lado $7^2 = 49$ não divide $a_0 = 7$. Portanto o polinômio f é irredutível em $\mathbb{Q}[X]$.

EXERCÍCIOS

34. Representar cada um dos seguintes polinômios, de $A[X]$, na forma de produto de uma constante por um polinômio primitivo:

a) $3X^2 + 6X + 6$, $A = \mathbb{Z}$

b) $2X^2 + 2X + 1$, $A = \mathbb{R}$

c) $2X^2 + (1+i)X + (1-i)$, $A = \mathbb{Z}[i]$

d) $2X^2 + (2 - \sqrt{2})X + 4$, $A = \mathbb{Z}[\sqrt{2}]$

35. Representar os polinômios abaixo, todos de $K[X]$, como produto de um elemento de K por um polinômio primitivo de $A[X]$ (onde K é o corpo de frações do anel de integridade A).

a) $\frac{1}{3} X^2 + \frac{1}{2} X + 6$, $A = \mathbb{Z}$

b) $\frac{1}{2} X^2 - \frac{5}{1-i} X + 2$, $A = \mathbb{Z}[i]$

c) $\frac{1}{4} X^2 + \frac{1}{2} X + \frac{1}{4 - 2\sqrt{2}}$, $A = \mathbb{Z}[\sqrt{2}]$

36. Mostre que um elemento primo p de um anel fatorial A, também é primo em $A[X]$.

37. Dê um exemplo que mostre ser falsa a recíproca do Lema 2 (Gauss).

38. Aplique o critério de Eisenstein aos seguintes polinômios de $\mathbb{Z}[X]$:

a) $2 + 2X + 4X^2 + X^3$

b) $X^5 - 7$

39. Mesmo exercício com

a) $X^4 - 2iX^3 + (1+i)X^2 + 4X + (1-i) \in A[X]$, onde $A = \mathbb{Z}[i]$;

b) $Y^3 + (2X+2)Y + (X+1) \in A[Y]$, onde $A = \mathbb{Z}[X]$;

c) $X^3 + 3X^2Y^2 + 2Y^2 + X^2Y + 7X \in A[Y]$, com $A = \mathbb{Z}[X]$.

40. a) Sendo A um anel de integridade, mostre que φ: $A[X] \longrightarrow A[X]$ dada por $\varphi(a_0 + a_1 X + \ldots) = a_0 + a_1 (X+1) + \ldots$ é um automorfismo de anéis.

b) Levando em conta a parte anterior, mostre que são irredutíveis sobre $\mathbb{Q}$ os seguintes polinômios de $\mathbb{Z}[X]$.

(I) $1 + X^2$

(II) $1 + X + \ldots + X^{p-2} + X^{p-1}$, onde p é um número primo positivo.

41. a) Considere o homomorfismo $\varphi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}_p[X]$ (p = número inteiro positivo qualquer) dado por $\varphi(a_0 + a_1 X + \ldots) = \overline{a}_0 + \overline{a}_1 X + \ldots$. Sendo $\bar{f} = \varphi(f)$ irredutível em $\mathbb{Z}_p[X]$, mostre que f é irredutível em $\mathbb{Z}[X]$

b) Aplique a parte (a) para concluir que são irredutíveis em $\mathbb{Z}[X]$

(I) $f = 1 + X + X^2 + X^3 + X^4$
Sugestão: $p = 2$

(II) $f = 8 + 11X + 6X^2 + X^3$.

Tais polinômios são irredutíveis em $\mathbb{Q}[X]$? Por que?

42. Use o corolário do lema 4 para concluir que o anel $\mathbb{Z}[\sqrt{-3}]$ não é fatorial.

Sugestão: Considerar o polinômio
$f = X^2 + (2 + \sqrt{-3})X + (-2 + \sqrt{-3}) \in (\mathbb{Z}[\sqrt{-3}])[X]$.

43. Dê um exemplo de um anel fatorial que não é principal.

44. Seja A um anel fatorial e K seu corpo de frações. Dê um exemplo de um polinômio $f \in A[X]$ que é irredutível em $K[X]$ sem o ser em $A[X]$.

45. Seja A um anel fatorial. Mostre que um divisor não constante de um polinômio primitivo $f \in A[X]$ também é primitivo.

46. Um corpo é um anel fatorial?

47. Se A é um anel fatorial, então $A[X_1, X_2, \ldots, X_n]$ é fatorial, $\forall\ n \geqslant 1$. Prove.

RESPOSTAS DE ALGUNS EXERCÍCIOS

CAPÍTULO 0

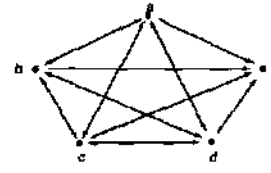
13. 3 14. 9 e 3

15. 07

CAPÍTULO I

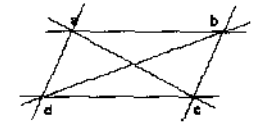
5. mn e 2^{mn}

8.



Nenhuma das quatro propriedades

9



$R = \{(ab, ab), (ab, cd), (cd, cd), (cd, ab), (ad, ad), (ad, bc), (bc, bc), (bc, ad), (ac, ac), (bd, bd)\}$

$\hat{R}$ é reflexiva, simétrica e transitiva.

11. reflexivas: R_1, R_2 e R_4
simétricas: R_1, R_4 e R_5
transitivas: R_1, R_4 e R_5
anti-simétricas: R_2, R_3 e R_5

13. Há relações simétricas e anti-simétricas.
Exemplo: $R = \{(a, a), (b, b)\}$ em $E = \{a, b\}$
Há relações não simétricas nem anti-simétricas.
Exemplo: $R = \{(a, b), (b, a), (b, c)\}$ em $E = \{a, b, c\}$

14. G_r contém a reta $y = x$, no caso em que R é reflexiva.
Quando R é simétrica G_r é uma figura (curva ou região) simétrica relativamente à reta $y = x$.

16. relações binárias: $2^{(n^2)}$

relações reflexivas: 2^{n^2-n}

relações simétricas: $2^{\frac{n(n+1)}{2}}$

20. R_1 e R_4

21. a

23. a

27. $A/R = \{\{0, 4, 8\}, \{1, 5, 9\}, \{2, 6, 10\}, [3, 7]\}$

29. $E/R = \{\{-3, -2, -1, 0\}, \{1\}, \{2\}, \{3\}\}$

30. $\overline{1} = Z$

31. $(\overline{\frac{1}{2}}) = \mathbb{Q}$

$(\overline{\sqrt{2}}) = \{\sqrt{2} + r \mid r \in \mathbb{Q}\}$

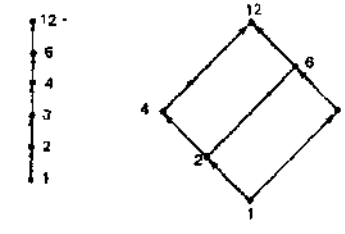
32. $\overline{1+i} = \{x + yi \mid x^2 + y^2 = 2\}$

33. $\mathbb{C}/\mathcal{R}$ é o feixe de retas de equação $y = k$, isto é paralelas ao eixo real.

34. a) π/R é o conjunto das curvas de equação $xy = k$, $k \in \mathbb{R}$.
b) π/S é o conjunto das curvas de equação $x - y = k$, $k \in \mathbb{R}$.
c) π/T é o conjunto das curvas de equação $x^2 + y^2 = k$, $k \in \mathbb{R}_+$.
d) π/V é o conjunto das curvas de equação $k_1x^2 + k_2y^2 = c$, $c \in \mathbb{R}_+$.

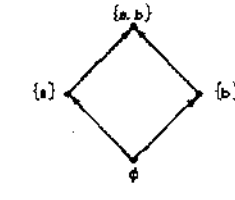
38. 15

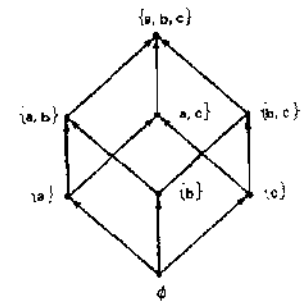
41. a) b)



42. a, c sim
b, d não

43.





45. $\ell \cdot s \cdot B = 30$
$\ell \cdot i \cdot B = 2$
$\inf B = 2$

$\sup B = 30$
$\nexists$ max B
$\nexists$ min B

46. $\ell \cdot s \cdot A = \{a, b, c, d\}, \{a, b, c, d, e\}$
$\ell \cdot i \cdot A = \{a\}, \{b\}$
$\nexists$ inf A
$\sup A = \{a, b, c, d\}$
$\max A = \{a, b, c, d\}$
$\nexists$ min A

47. $\ell \cdot s = \{L \in \mathbb{Q} \mid L > \sqrt{2}\}$
$\ell \cdot i = \{\ell \in \mathbb{Q} \mid \ell < -\sqrt{2}\}$
$\nexists$ inf, sup, max, min

48. $\ell \cdot s = 1, h, i$
$\ell \cdot i = b$
$\inf = b$
$\sup = f$
max
min
$R^{-1} = \{(a, a), (b, b), (c, c), \ldots, (j, j), (d, a), (d, b), (e, b), (e, c), (f, d), (f, e), (g, e), (h, f), (i, f), (i, g), (j, g), (f, a), (h, e), (i, a), (f, b), (h, b), (i, b), (g, b), (j, b), (f, c), (g, c), (h, c), (i, c), (j, c), (h, d), (i, d), (h, e), (i, c), (j, e)\}$

49. $\ell \cdot s = \{(x, y) \mid 2 \mid x \text{ e } 2 \leqslant y$
$\ell \cdot i = (1, 1)$ e $(1, 0)$
$\inf = (1, 1)$
$\sup = (2, 2)$
$\nexists$ min
$\nexists$ max

52. R_2 e R_4

54. n^m

55. $f = \{(0, 1), (1, 1), (\frac{1}{2}, 1), (\sqrt{2}, -1), (\pi, -1), (\frac{7}{3}, 1)\}$

56. 1, 4, 1, 5, 0 respectivamente

57. $-1, \frac{25}{3}, -2, 5\sqrt{2}, \frac{-4\pi + 25}{5}$ respectivamente

58. só no 1º e 2º

59. $\{7, 8\}, \{7, 8\}, \{6, 8, 9\}, \{6, 7, 8, 9\}, \{0, 1, 3, 4\}$ e $\{5\}$ respectivamente

60. $1, 3, \sqrt{2}, -1,]0, 1[, [0, 2], \mathbb{R}_+^*, [-3, 3], [-3, 3]$ e ϕ respectivamente

61. $[0, 2], \mathbb{R}_+^*, \mathbb{R}_+^*, [-1, 1, -4, 16^3], [-4, 16^3], \phi$ respectivamente.

62. $[0, 1], [-1, 1], [-1, 1], \{x \in \mathbb{R} \mid x = \pm \frac{\pi}{3} + 2k\pi\}$,
$\{x \in \mathbb{R} \mid -\frac{\pi}{3} + 2k\pi \leqslant x \leqslant \frac{\pi}{3} + 2k\pi\}$,
$\{x \in \mathbb{R} \mid -\frac{\pi}{2} + 2k\pi \leqslant x \leqslant \frac{3\pi}{2} + 2k\pi\}$
respectivamente

64. f_1 e f_3

65. f_2 e f_3

68. injetoras: $A_{n,m}$ se $n \geqslant m$;
0 se $n < m$
sobrejetora: 0 se $n > m$;
se $n \leqslant m$, há a fórmula de recorrência
$S_{m,n} = n^m - \binom{n}{1} S_{m,n-1} - \binom{n}{2} S_{m,n-2} - \ldots - \binom{n}{n-1} S_{m,1}$

70. injetoras: e, c, f
sobrejetoras: a, f, g

71. a) $f(x) = 2^x$, $A = \mathbb{R}$, $B = \mathbb{R}_+^*$
b) $f(x) = \frac{1}{x}$, $A = \mathbb{R}^*$ e $B = \mathbb{R}$
c) $f(x) = \text{sen } x$, $A = \mathbb{R}$ e $B = [-1, 1]$
d) $f(x) = \text{tg } x$, $A = \{x \mid x \neq \frac{\pi}{2} + k\pi\}$, $B = \mathbb{R}$

72. $f^{-1}: \mathbb{R} \longrightarrow \mathbb{R}$ é tal que $f^{-1}(x) = \frac{x - b}{a}$

73. $f^{-1}: \mathbb{R} - \{\frac{a}{c}\} \longrightarrow \mathbb{R} - \{-\frac{d}{c}\}$ é tal que
$f^{-1}(x) = \frac{b - dx}{cx - a}$

74. $f^{-1}: \mathbb{R} \longrightarrow]-1, 1[$ é tal que:
$$f^{-1}(x) = \begin{cases} \frac{x}{1 - x}, & \text{se } x < 0 \\ \frac{x}{1 + x}, & \text{se } x \geqslant 0 \end{cases}$$

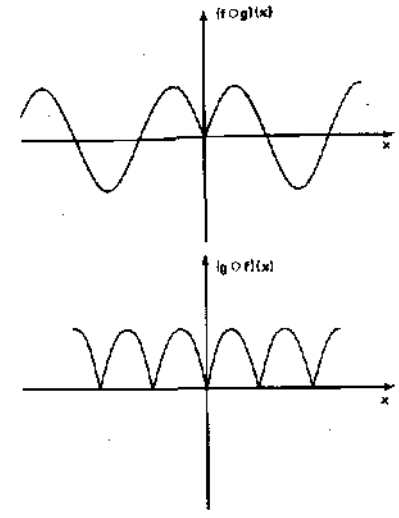
75. a) não
b) sim
c) $\{(x, y) \mid x = 0 \text{ ou } y = 0\}$
d) $[0, 1]$
e) $\mathbb{R}_+$

79. $g \circ f = \{(1, 8), (2, 8), (3, 8)\}$
nem injetora nem sobrejetora

80. $g \circ f = \{(a, a), (b, c), (c, c), (d, d)\}$
$f \circ g = \{(a, c), (b, b), (c, c), (d, d)\}$
$g \circ h = \{(a, a), (b, d), (c, a), (d, d)\}$
$h \circ f = \{(a, d), (b, b), (c, b), (d, d)\}$
$h \circ h = \{(a, d), (b, d), (c, d), (d, d)\}$

81. $(f \circ g)(x) = x^2 + 1$
$(f \circ h)(x) = x$
$(g \circ h)(x) = x^2 + 2x + 3$
$(g \circ f)(x) = x^2 - 2x + 3$
$(h \circ f)(x) = x$
$(h \circ g)(x) = x^2 + 3$

82. $(f \circ g)(x) = x^6 + 3x^4 + 3x^2 + 2$
$(g \circ f)(x) = x^6 + 2x^3 + 2$
$(f \circ f)(x) = x^9 + 3x^6 + 3x^3 + 2$
$(g \circ g)(x) = x^4 + 2x^2 + 2$

83.


85. $(f \circ g)(x) = \begin{cases} 2(1 - x), & \text{se } x < 1 \\ 2(1 + x), & \text{se } x \geqslant 1 \end{cases}$
$(g \circ f)(x) = \begin{cases} 1 + x^2, & \text{se } x \leqslant -1 \\ 1 - x^2, & \text{se } -1 < x < 0 \\ 1 - 2x, & \text{se } 0 < x < \frac{1}{2} \\ 1 + 2x, & \text{se } x \geqslant \frac{1}{2} \end{cases}$

86. $(f \circ g)(x) = \begin{cases} 9x^2 + 1, & \text{se } x < 0 \\ 6x + 1, & \text{se } 0 \leqslant x < 1 \\ 14x + 3, & \text{se } 1 \leqslant x \leqslant 5 \\ 2x + 5, & \text{se } x > 5 \end{cases}$
$(g \circ f)(x) = \begin{cases} x^2 + 3, & \text{se } x < -2 \\ 7x^2 + 8, & \text{se } -2 \leqslant x \leqslant 2 \\ 14x + 8, & \text{se } 0 < x \leqslant 2 \\ 2x + 3, & \text{se } x > 2 \end{cases}$

87. $(f \circ f)(x) = \begin{cases} x + 2, & \text{se } x \leqslant -1 \\ -1 - 2x, & \text{se } -1 < x \leqslant 0 \\ -1 + 4x, & \text{se } 0 < x \leqslant \frac{1}{2} \\ 2 - 2x, & \text{se } x > \frac{1}{2} \end{cases}$

88. $n = 2$ e $a = \sqrt[3]{3}$

89. $g(x) = 2x^2 - x - 2$

90. $(f \circ g)(x) = x$
$(g \circ f)(x) = x$
então $g = f^{-1}$

91. a) $g(x) = x - 1$, se $x \geqslant 1$ e $g(0) = k \in \mathbb{R}$
f não é sobrejetora
b) $f(x) = 2x$ se $x \leqslant k$ e $f(x) = 2x + 1$, se $x > k$.
g não é injetora

92. c, e

96. g, i

97. f, $\mathbb{R}$

98. $[0, 2[$ e $[0, 1]$ respectivamente

99. R^2 e ϕ

100. $\{(x, y) \in R^2 \mid x^2 + y^2 \geqslant 1\}$ e ϕ respectivamente

101. associativas: c, d, f, g, m, n, o, p, q, r
comutativas: a, c, d, f, g, k, l, m, n, o, p, q, r
têm neutro: c, d, f, g, l, p
elementos simetrizáveis:
c) 0 d) $x \mid x \in \mathbb{R}$ f) 0 g) 0 e -2
l) $x \mid x \geqslant -\frac{1}{2}$ p) 0

102. associativas: a, b, c, d, e
comutativas: a, b, c, d, e
têm neutro: b, c, d, e
elementos simetrizáveis:
b) $(x, y) \mid x, y \in \mathbb{Z}$
c) $(x, y) \mid x = \pm 1$ e $y \in \mathbb{Z}$
d) $(x, y) \mid x \in \mathbb{Z}$ e $y = \pm 1$
e) (1, 0), (0, 1), (-1, 0) e (0, -1)

103. $U_s(\mathbb{Z}^3) = \{(x, y, z) \mid x, y, z \in \{-1, 1\}\}$

104. a) $m^2 = m$ e $n^2 = n$
b) $m = n$
c) $m = n = 1$

105. $a = b = 0$ e $c \neq 0$ ou
$a = b = 1$ e c qualquer

106. $e = \begin{pmatrix} 1 & \alpha \\ 0 & 0 \end{pmatrix}$ com $\alpha \in \mathbb{R}$

107. a) $\mathbb{R}$; b) ϕ; c) $\mathbb{R}_+$; d) $\mathbb{R}$; e) $\mathbb{R}^*$; f) $\mathbb{R}_+ - \{1\}$;
g) $\mathbb{Z} - \{-1\}$; h) $\mathbb{Z}^*$; i) $\mathbb{Q}^*$; j) $\mathbb{Z}^*$; k) ϕ; l) $\{0\}$;
m) ϕ; n) ϕ; o) ϕ; p) $\{0\}$; q) ϕ; r) ϕ

108. a) não existe
b) $(x, y) \mid x \in \mathbb{Z}$, $y \in \mathbb{Z}$
c) $(x, y) \mid x \neq 0$ e $y \in \mathbb{Z}$
d) $(x, y) \mid x \in \mathbb{Z}$ e $y \neq 0$
e) $(x, y) \mid x \in \mathbb{Z}^*$ ou $y \in \mathbb{Z}^*$

111. não existe

112. a, b, d

113. b, c, d

118.

∘	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_3	f_4	f_1
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_1	f_2	f_3

f_3, f_1, f_2, f_4 e f_2 respectivamente

122. comutativas: a, c
têm neutro: a, b, c
elementos simetrizáveis:
a) a, b, c, d
b) b
c) todos

123.

*	a	b	c	d
a	a	b	c	d
b	b	d	a	c
c	c	a	d	b
d	d	c	b	a

124.

*	e	a	b	c
e	e	a	b	c
a	a	a	a	a
b	b	a	c	e
c	c	e	e	b

125. Em $\mathbb{R}_+$, $x * y = \sqrt{x^2 + y^2}$

126.

	e	a	b	c
e	e	a	b	c
a	a	b	e	e
b	b	e	c	e
c	c	e	e	a

127.

	e	a	b	c
e	e	a	b	c
a	a	b	e	e
b	b	c	e	a
c	c	b	a	e

128.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	b	e	e
c	c	a	e	c

129. $X \subset Y$ ou $Y \subset X$

130. $\{1, 2, 4\}$, $\{1, 2, 6\}$, $\{1, 2, 12\}$, $\{1, 3, 6\}$, $\{1, 3, 12\}$, $\{1, 4, 12\}$, $\{1, 6, 12\}$, $\{2, 3, 6\}$, $\{2, 4, 12\}$, $\{2, 6, 12\}$, $\{3, 4, 12\}$ $\{2, 4, 12\}$, $\{2, 6, 12\}$, $\{3, 4, 12\}$, $\{3, 6, 12\}$, $\{4, 6, 12\}$

CAPÍTULO II

4. a) é grupo
b) não é, pois $U_{\mathbb{Z}\times\mathbb{Z}} = \{(1, -1), (1, 1), (-1, 1), (-1, -1)\}$

5. $(\mathbb{R}^A, \cdot)$ não é grupo, pois:
$U_{(\mathbb{R}^A)} = \{f : A \longrightarrow \mathbb{R} \mid f(x) \neq 0, \forall x \in A\}$

9.

	e	a
e	e	a
a	a	e

10.

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

12.

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

14.

	e	a	a^2	a^3
e	e	a	a^2	a^3
a	a	a^2	a^3	e
a^2	a^2	a^3	e	a
a^3	a^3	e	a	a^2

15.

	e	a	a^2	a^3	a^4	a^5
e	e	a	a^2	a^3	a^4	a^5
a	a	a^2	a^3	a^4	a^5	e
a^2	a^2	a^3	a^4	a^5	e	a
a^3	a^3	a^4	a^5	e	a	a^2
a^4	a^4	a^5	e	a	a^2	a^3
a^5	a^5	e	a	a^2	a^3	a^4

6.

	e	a	a^2	a^3	b	ba	ba^2	ba^3
e	e	a	a^2	a^3	b	ba	ba^2	ba^3
a	a	a^2	a^3	e	ba^3	b	ba	ba^2
a^2	a^2	a^3	e	a	ba^2	ba^3	b	ba
a^3	a^3	e	a	a^2	ba	ba^2	ba^3	b
b	b	ba	ba^2	ba^3	e	a	a^2	a^3
ba	ba	ba^2	ba^3	b	a^3	e	a	a^2
ba^2	ba^2	ba^3	b	ba	a^2	a^3	e	a
ba^3	ba^3	b	ba	ba^2	a	a^2	a^3	e

8.

*	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	c	d	f	e
b	b	c	d	f	e	a
c	c	d	f	e	a	b
d	d	f	e	a	b	c
f	f	e	a	b	c	d

9. são subgrupos: a, b, c, d, f, g, h, i,
7. b) são subgrupos: H_1 e H_2
9. $\{0\}$, $\{0, 2\}$ e $\mathbb{Z}_4$
0. $\{a, c\}$ e $\{e, b, d\}$
1. $\{e, c\}$, $\{e, f\}$ e $\{a, e, b\}$
5. são homomorfismos: $1^{\underline{o}}$, $2^{\underline{o}}$, $4^{\underline{o}}$, $5^{\underline{o}}$ e $6^{\underline{o}}$
7. injetores: $1^{\underline{o}}$ (se $k \neq 0$), $4^{\underline{o}}$ e $6^{\underline{o}}$
sobrejetores: $5^{\underline{o}}$ e $6^{\underline{o}}$
8. $1^{\underline{o}}$) $\{0\}$ se $k \neq 0$, ou $\mathbb{Z}$ se $k = 0$
$2^{\underline{o}}$) $\{1, -1\}$
$4^{\underline{o}}$) $\{0\}$
$5^{\underline{o}}$) $\{(0, y) \mid y \in \mathbb{Z}\}$
$6^{\underline{o}}$) $\{0\}$
9. $N(f) = \{(x, y) \in \mathbb{Z}\times\mathbb{Z} \mid x = y\}$
3. São homomorfismos: I, II, III, IV, e VII
Núcleos: II) $\{1, -1\}$
III) $\{\cos\theta + i \operatorname{sen}\theta \mid \theta \in \mathbb{R}\}$
IV) $\{1\}$
V) $\{1, -\frac{1}{2} + i\frac{\sqrt{3}}{2}, -\frac{1}{2} - i\frac{\sqrt{3}}{2}\}$
1. $f(2\mathbb{Z}) = \{1, -1\}$
$f(3\mathbb{Z}) = \{1, -i, -1, i\}$
2. $f^{-1}(\{1, -1\}) = 2\mathbb{Z}$

45.

*	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	e
c	c	e	a	b

$a^2 = b$, $b^{-3} = b$, $x = e$

46.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

55. $f_1 = \{(e, e), (e, a), (b, b), (c, c)\}$
$f_2 = \{(e, e), (a, b), (b, c), (c, b)\}$
$f_3 = \{(e, e), (a, b), (b, a), (c, c)\}$
$f_4 = \{(e, e), (a, b), (b, c), (c, a)\}$
$f_5 = \{(e, e), (a, c), (b, b), (c, a)\}$
$f_6 = \{(e, e), (a, c), (b, a), (c, b)\}$

60. Todas são homomorfismos
Núcleos: I) $\{(e_G, y) \mid y \in J\}$
II) $\{(x, e_J) \mid x \in G\}$
III) $\{e_G\}$
IV) $\{(e_G, e_J)\}$
V) $\{e_J\}$

61. $[-1]_{\mathbb{Z}} = \mathbb{Z}$, $[3]_{\mathbb{Z}} = 3\mathbb{Z}$,
$[3] = \{\ldots, 3^{-2}, 3^{-1}, 1, 3, 3^2, \ldots\}$
$[i] = \{1, i, -1, -i\}$.

63. cíclico: $\mathbb{Z}_4$
não cíclico: grupo de Klein

67. $[b] = \{a, b, d\}$
$o(d) = 3$
geradores de G: a, f
$x = c$

68. $[b] = \{e, b, d, g\}$
$o(d) = 2$
G não é cíclico
$x = h$

84. H e $\overline{1} + H$

85. $3\mathbb{Z}$, $1 + 3\mathbb{Z}$, $2 + 3\mathbb{Z}$

86. H, $f_2 \circ H$ e $f_3 \circ H$ à esquerda com
$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ e $f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$
H, $H \circ f_2$ e $H \circ f_4$ com
$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

88. É finito porque
$(a, b) \sim (c, d) \Rightarrow a - b \in \mathbb{Z}$ e $b \equiv d \pmod 2$
então
$\mathbb{Z}\times\mathbb{Z}/_{\mathbb{Z}\times 2\mathbb{Z}} = \{\overline{(0,0)}, \overline{(0,1)}\}$

89. Há infinitas classes do tipo $(n, \overline{0}) + H$ com $n \in \mathbb{Z}$ e $0 \in \mathbb{Z}_2$

97. $\mathbb{Z} + (-1) = \mathbb{Z}$
$\mathbb{Z} + \frac{1}{2} = \left\{ \frac{2n+1}{2} \mid n \in \mathbb{Z} \right\}$

104. $H = \{e, a^2, a^4\}$
$G/H = \{H, aH\}$

	H	aH
H	H	aH
aH	aH	H

105. $H = \{\overline{0}, \overline{3}\}$
$G/H = \{H, \overline{1}+H, \overline{2}+H\}$

+	H	$\overline{1}+H$	$\overline{2}+H$
H	H	$\overline{1}+H$	$\overline{2}+H$
$\overline{1}+H$	$\overline{1}+H$	$\overline{2}+H$	H
$\overline{2}+H$	$\overline{2}+H$	H	$\overline{1}+H$

$H = \{\overline{0}, \overline{2}, \overline{4}\}$
$G/H = \{H, \overline{1}+H\}$

+	H	$\overline{1}+H$
H	H	$\overline{1}+H$
$\overline{1}+H$	$\overline{1}+H$	H

106.

$\mathbb{Z}_6/H$

+	H	$\overline{1}+H$	$\overline{2}+H$	$\overline{3}+H$	$\overline{4}+H$
H	H	$\overline{1}+H$	$\overline{2}+H$	$\overline{3}+H$	$\overline{4}+H$
$\overline{1}+H$	$\overline{1}+H$	$\overline{2}+H$	$\overline{3}+H$	$\overline{4}+H$	H
$\overline{2}+H$	$\overline{2}+H$	$\overline{3}+H$	$\overline{4}+H$	H	$\overline{1}+H$
$\overline{3}+H$	$\overline{3}+H$	$\overline{4}+H$	H	$\overline{1}+H$	$\overline{2}+H$
$\overline{4}+H$	$\overline{4}+H$	H	$\overline{1}+H$	$\overline{2}+H$	$\overline{3}+H$

$\mathbb{Z}/_{2\mathbb{Z}}$

+	$\mathbb{Z}$	$1+2\mathbb{Z}$
$\mathbb{Z}$	$\mathbb{Z}$	$1+2\mathbb{Z}$
$1+2\mathbb{Z}$	$1+2\mathbb{Z}$	$\mathbb{Z}$

108.

+	$\overline{(0,0)}$	$\overline{(0,1)}$	$\overline{(1,0)}$	$\overline{(1,1)}$	$\overline{(2,0)}$	$\overline{(2,1)}$
$\overline{(0,0)}$	$\overline{(0,0)}$	$\overline{(0,1)}$	$\overline{(1,0)}$	$\overline{(1,1)}$	$\overline{(2,0)}$	$\overline{(2,1)}$
$\overline{(0,1)}$	$\overline{(0,1)}$	$\overline{(0,0)}$	$\overline{(1,1)}$	$\overline{(1,0)}$	$\overline{(2,1)}$	$\overline{(2,0)}$
$\overline{(1,0)}$	$\overline{(1,0)}$	$\overline{(1,1)}$	$\overline{(2,0)}$	$\overline{(2,1)}$	$\overline{(0,0)}$	$\overline{(0,1)}$
$\overline{(1,1)}$	$\overline{(1,1)}$	$\overline{(1,0)}$	$\overline{(2,1)}$	$\overline{(2,0)}$	$\overline{(0,1)}$	$\overline{(0,0)}$
$\overline{(2,0)}$	$\overline{(2,0)}$	$\overline{(2,1)}$	$\overline{(0,0)}$	$\overline{(0,1)}$	$\overline{(1,0)}$	$\overline{(1,1)}$
$\overline{(2,1)}$	$\overline{(2,1)}$	$\overline{(2,0)}$	$\overline{(0,1)}$	$\overline{(0,0)}$	$\overline{(1,1)}$	$\overline{(1,0)}$

$G/(3\mathbb{Z}\times 2\mathbb{Z})$

+	$\mathbb{Z}\times\mathbb{Z}$
$\mathbb{Z}\times\mathbb{Z}$	$\mathbb{Z}\times\mathbb{Z}$

$G/(2\mathbb{Z}\times 2\mathbb{Z})$

CAPÍTULO III

5. $a = 1$, $b = c = -2$, $d = 6$
Sim

6.

*	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

*	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	c	a
d	a	d	a	d

7. $\mathcal{P}\{a, b\}$

16. a, c, d

17. são subanéis: a, c, d

18. L_1, L_2 e L_3

19. a) $A = \mathbb{Q}$ e $B = \mathbb{Z}$
b) $A = \mathbb{Z}\times\mathbb{Z}$ e $B = \mathbb{Z}\times\{0\}$
c) $A = \mathbb{Z}$ e $B = 2\mathbb{Z}$
d) $A = \mathbb{Z}\times 2\mathbb{Z}$ e $B = \mathbb{Z}\times\{0\}$
e) $A = 2\mathbb{Z}$ e $B = 4\mathbb{Z}$

20. $\{\overline{0}\}$, $\{\overline{0}, \overline{3}\}$, $\{\overline{0}, \overline{2}, \overline{4}\}$ e $\mathbb{Z}_6$

21. $\{\emptyset\}$, $\mathcal{P}(\{a, b\})$, $\mathcal{P}(\{a, c\})$, $\mathcal{P}(\{b, c\})$ e $\mathcal{P}(\{a, b, c\})$

24. inversíveis a) $\{1, -1\}$; b) $\mathbb{Q}^*$; c) $\mathbb{Z}^*\times\mathbb{Z}^*$; d) $\{(1, 1), (1, -1), (-1, 1), (-1, -1)\}$; d) $\mathbb{Z}\mathbb{Z}$; e) $\{\overline{1}, \overline{3}\}$; f) $\{\overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{11}, \overline{13}\}$; g) $\{A \in M_2(\mathbb{R}) \mid \det A \neq 0\}$; h) $\{(\overline{1}, \overline{1}), (\overline{1}, \overline{2})\}$
regulares
a) $\mathbb{Z}^*$; b) $\mathbb{Q}^*$; c) $\mathbb{Z}^*\times\mathbb{Z}^*$; d) e) f) g) h) idem inversíveis.

26. a) $\mathbb{Q} - \{1\}$
b) $\{(x, y) \in \mathbb{Z}\times\mathbb{Z} \mid x = \pm 1\}$

28. $\mathbb{Z}_2$

29. a) $\{\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}\}$
b) $(\overline{3}, \overline{2})$

31. $N(\mathbb{Z}) = \{\overline{0}\}$
$N(\mathbb{Z}_6) = \{\overline{0}\}$
$N(\mathbb{Z}_8) = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$
$N(\mathbb{Z}_2\times\mathbb{Z}_4) = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{2})\}$
$N(\mathbb{R}^{\mathbb{R}}) = \{f \in \mathbb{R}^{\mathbb{R}} \mid f(x) = 0, \forall x\}$

42. são subcorpos: b, c

43. é subcorpo: a

47. É verdadeiro. Uma família de subcorpos de $\mathbb{R}$ é formada pelos conjuntos da forma $\mathbb{Q}[\sqrt{p}]$, p primo e inteiro $\mathbb{Q}[\sqrt{p}] = \{x + y\sqrt{p} \mid x, y \in \mathbb{Q}\}$.

48. São homomorfismos: 3°, 4°, 5°, 6° e 7°

49. Núcleos: 3°) $\{0\}$; 4°) $\{(0, y) \mid y \in \mathbb{Z}\}$; 5°) $(0, 0)$; 6°) $\{x \in \mathbb{Z} \mid x \equiv 0 \pmod n\}$; 7°) $\{0\}$

50. Homomorfismos: a, b, e.
Núcleos: a) $\{(x, 0) \mid x \in \mathbb{Z}\}$
b) $\{(x, 0) \mid x \in \mathbb{Z}\}$
c) $\{0\}$

51. $A = B = \mathbb{Z}\times\mathbb{Z}$ e $f(x, y) = (x, 0)$

53. $f_1(x) = (0, 0)$, $f_2(x) = (x, 0)$, $f_3(x) = (0, x)$ e $f_4(x) = (x, x)$

64. Há 9 possibilidades:
1) $m = n = p = q = 0$
2) $m = p = q = 0$ e $n = 1$
3) $n = p = q = 0$ e $m = 1$
4) $m = n = p = 0$ e $q = 1$
5) $m = n = q = 0$ e $p = 1$
6) $m = p = 0$ e $n = q = 1$
7) $m = q = 0$ e $n = p = 1$
8) $n = p = 0$ e $m = q = 1$
9) $n = q = 0$ e $m = p = 1$
f é automorfismo nos casos: 7 e 8

65. $f_1(x) = \overline{0}$ e $f_2(x) = \overline{x}$

66. $f_1(x) = \overline{0}$, $f_2(x) = \overline{x}$, $f_3(x) = \overline{3x}$ e $f_4(x) = \overline{4x}$

67. São ideais a, b, c, e, g, i, j.

68. É ideal à esquerda: L_4

70. a) $\{\overline{0}, \overline{2}, \overline{4}\}$ e) $\mathbb{Z}_8$
b) $5\mathbb{Z}$ f) $4\mathbb{Z}$
c) $\mathbb{Q}$ g) $\mathbb{R}$
d) $\mathbb{R}$ h) $\mathbb{C}$

71. $\{\overline{0}\}$; $\{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$; $\{\overline{0}, \overline{4}\}$ e $\mathbb{Z}_6$

73. b) $J = \{\overline{0}, \overline{6}\}$

74. b) 5 e -5

80. $\langle 12\rangle + \langle 21\rangle = \langle 3\rangle$
$\langle 12\rangle \cap \langle 21\rangle = \langle 84\rangle$

81. $\langle 12, 20, 28\rangle = \langle 4\rangle = \langle -4\rangle$

83. $\langle\langle 4\rangle, 6\rangle = \langle 2\rangle$

86. $\langle X\rangle$ em $\mathbb{Z}[X]$

99. $A = \mathbb{Z}$, $I = 4\mathbb{Z}$ e $A/I = \mathbb{Z}_4$

103. a) 3; b) 0; c) 0; d) 0; e) 24; f) 0

104. 0

108. $\mathbb{Z}_m$

109. Não, pois $1 \cdot_A = 1_A \neq 0_A$

CAPÍTULO IV

1. X, $X + \overline{1}$, $X + \overline{2}$, $\overline{2}X$, $\overline{2}X + \overline{1}$, $\overline{2}X + \overline{2}$; $(n-1) \cdot nP$; n^2

2. a) X
b) $2 + 3X + 2X^2 + 2X^3$
c) $X^3 + 2X$
d) $1 + X^2 + X^4$
e) $1 + 2X^{18}$

3. $f + g + h = (-3, 1) + (1, 0)X + (1, 1)X^2$
$fg - h^2 = (-16, -1) + (-7, 0)X + (-1, 1)X^2 + (2, 0)X^3$
$fh + g = (-4, -2) + (-9, 1)X + (-3, 1)X^2$

6. a) 10; b) 12; c) 28; d) 0

8. $a = 4$ e $b = 4$

9. a) $a = \frac{p^2}{q^2}$ com $p, q \in \mathbb{Z}$ e $q \neq 0$
b) $a \in \mathbb{R}_+$; c) a qualquer

10. $\partial(f + g) = 4$, $\partial(f - g) = 3$, $\partial f^3 = 12$, $\partial g^2 = 6$ e $\partial(f + g)^3 = 12$

11. $\partial(fg) = 10$; $\partial(f^2 - g^2) = 7$, $\partial(f^2 + g^2) \leqslant 10$

12. $f = 1 + 4X$

14. $a = 1$, $b = -1$, $c = 4$ e $f^{-1} = \frac{1}{2}$

16. $A[X]$ certamente não é corpo

17. 1°) $gr\, q = 2$ e $gr\, r \leqslant 3$
2°) $gr\, q = 1$ e $gr\, r \leqslant n - 1$
3°) se $n < m$, então $q = 0$ e $r = n$
4°) se $n \geqslant m$, então $gr\, q = n - m$ e $gr\, r \leqslant m$

18. 1°) $q = r = 0$
2°) $q = 0$ e $r = X^2 - 1$
3°) $q = 4X^2 + 4$ e $r = -6X + 2$
4°) $q = 6X$ e $r = 4X^2 + 3X + 2$
5°) $q = X^6 - X^5 - 3X^4 + 8X^3 + 7X^2 - 11X - 6$, $r = 9X^3 + 5X + 6$

19. a) $q = 0$ e $r = X + 1$
b) $q = (1, 2)X - (0, 2)$ e $r = (1, 3)$
c) $q = (1, 1)X + (1, 1)$ e $r = (0, 0)$
d) $q = nX^{n-1} + (n-1)X^{n-2} + \ldots + 1$ e $r = 0$

20. $a = 6$

21. $a = -\frac{63}{6}$, $b = \frac{72}{5}$, $c = 0$

22. $a = 8$ e $b = -6$
$q = X^2 + 2X - 1$

23. $a = 10$ e $b = -11$

26. $k = \{0, 1\}$

27. geradores de I : X e $-X$
geradores de J : 2 e -2

28. Impossível

29. $1 + X^4 = (1 + \sqrt{2}\,X + X^2)(1 - \sqrt{2}\,X + X^2)$
Não pois f não tem raiz real

34. São subanéis : a e b
são ideais : a e b

38. 0

40. $r = 2X^3 + 3X^2 - 3X - 2$

41. $f = 3X^5 + X^4 + 5X^2 + 5X + 1$

42. $f = X^4 - 5X^2 + 6$

43. não existe f

47. $r = 2$

51. i) $q = X^3 - X^2 + 2X^2 + 12$ e $r = 34$
ii) $q = X^2 + X - 1$ e $r = 1$
iii) $q = (3, 0)X^2 + (-3, 0)X + (5, 0)$ e $r = (-4, 0)$

52. 1º) $q = X^{n-1} + X^{n-2} + X^{n-3} + \ldots + X + 1$ e $r = 0$
2º) $q = X^{n-1} - X^{n-2} + X^{n-3} - \ldots + (-1)^{n-1}$ e $r = 0$ (se n ímpar) ou $r = 2$ (se n par)

59. a) $d = 1$
b) $d = (X + 1)^2$
c) $d = X + 1$

68. Em $\mathbb{Z}[X]$, $f = 4(1 + 2X^2)$ é redutível
Em $\mathbb{R}[X]$, f é irredutível pois 4 é inversível
Em $\mathbb{C}[X]$, $f = 4(\frac{1}{2} + \sqrt{2}\,X)(\frac{1}{2} + i\sqrt{2}\,X)$ é redutível

75. Em $\mathbb{Q}[X]$, $f = (X^2 + 2)(X^2 - 2)$
Em $\mathbb{R}[X]$, $f = (X^2 + 2)(X + \sqrt{2})(X - \sqrt{2})$
Em $\mathbb{C}[X]$, $f = (X + i\sqrt{2})(X - i\sqrt{2})(X + \sqrt{2})(X - \sqrt{2})$

76. $X^4 + 4 = (X^2 + 2X + 2)(X^2 - 2X + 2)$

78. $f(-1) = 0 \therefore X + 1 \mid f$

84. $F = (2, 2X, 1, 0, 0, \ldots, 0, \ldots)$

85. $F = (1 + X)Y + X^4Y^2 + 2X^2Y^3$

86. $\partial F = 5$

CAPÍTULO VI

1. Não é simétrica pois $1 \mid 0$ e $0 \nmid 1$
Não é anti-simétrica se $A \neq \{0, 1\}$ pois
$\mu \in U(A)$, $\mu \neq 1$, $a \mid au$ e $au \mid a$ e $a \neq au$

3. a) $a \neq 0 \Longrightarrow \overline{a} = A^*$
$\overline{0} = \{0\}$
b) $a \neq 0 \Longrightarrow \overline{a} = \{a, -a\}$
$\overline{0} = \{0\}$
c) $a \in K^* \Rightarrow \overline{a} = K^*$
$\overline{0} = \{0\}$
$f \in K[X] - K \Longrightarrow \overline{f} = \{af \mid a \in K^*\}$

8. $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$
$U(\mathbb{Z}[\sqrt{-5}]) = \{1, -1\}$

14. $1, -1, i, -i, 1+i, 1-i, -1+i, -1-i, 2, -2, 2i, -2i$

15. possíveis mdc: $1+i, -1-i, 1-i, -1+i$

20. $5 = (1 + 2i)(1 - 2i)$
$3 + i = (2 - i)(1 + i)$
$4 = (1 + i)^2(1 - i)^2$
$2i = (1 + i)^2$
11 é irredutível

21. mdc $(3 + 6i, 2i) = 1$ ou -1 ou i ou $-i$
mdc$(4, 1 + i) = 1 + i$ ou $-1 - i$ ou $i - 1$ ou $-i + 1$

22. $(ac^{-1})c = a \Longrightarrow c \mid a$
$(bc^{-1})b = b \Longrightarrow c \mid b$
$\left.\begin{array}{l} c' \mid a \Longrightarrow r_1 c' = a = r_3 c \Rightarrow c = r_1^{-1} r_3 c' \\ c' \mid b \Longrightarrow r_2 c' = b = r_4 c \Longrightarrow c = r_2^{-1} r_2 c' \end{array}\right\} \Longrightarrow c' \mid c$

27. $10 = (2 + \sqrt{-6})(2 - \sqrt{-6})$
e mdc $(2 + \sqrt{-6}, 2 - \sqrt{-6}) \neq 1$

28. $8 = (1 + \sqrt{-7})(1 - \sqrt{-7})$
e mdc $(1 + \sqrt{-7}, 1 - \sqrt{-7}) \neq 1$

34. a) $3(X^2 + 2X + 2)$
b) $2X^2 + 2X + 1$ é primitivo em $\mathbb{R}[X]$
c) $(1 + i)((1 - i)X^2 + X - i)$
d) $\sqrt{2}\,(\sqrt{2}\,X^2 + (\sqrt{2} - 1)X + 2\sqrt{2})$

35. a) $\frac{1}{6}(2X^2 + 3X + 36)$

b) $\frac{1}{2}(X^2 - 5(1 + i)X + 4)$

c) $\frac{1}{4\sqrt{2} - 4}((\sqrt{2} - 1)X^2 + (2\sqrt{2} - 2)X + \sqrt{2})$

37. No anel $\mathbb{Z}[X]$, $X + 1$ é primitivo e não pode ser decomposto num produto de primitivos pois tem grau 1

38. a) $2 \mid 2, 2 \mid 4$, $2 \neq 1$ e $4 \neq 2$, então o polinômio é irredutível em $\mathbb{Q}[X]$
b) $7 \mid -7, 7 \mid 0, 7 \neq 1$ e $7^2 \nmid -7$ então o polinômio é irredutível em $\mathbb{Q}[X]$

39. a) $1 - i \mid 1 - i$, $1 - i \mid 4$, $1 - i \mid (1 + i, 1 - i \mid -2i$, $1 - i \nmid 1$ e $(1 - i)^2 \nmid 1 - i$:
b) $X + 1 \mid X + 1$, $X + 1 \mid 2X + 2$, $X + 1 \mid 0$, $X + 1 \nmid 1$ e $(X + 1)^2 \nmid X + 1$
c) $X \mid X^3 + 7X$, $X^1 \mid X^2$, $X \nmid 3X^2 + 2$ e $X^2 \nmid X^3 + 7X$

43. $\mathbb{Z}[X]$

44. $f = 2(X^2 - 2)$ é redutível em $\mathbb{Z}[X]$ e não o é em $\mathbb{Q}[X]$

47. Todo corpo K é um anel fatorial pois :
não existindo em K elementos não nulos e não inversíveis não há elementos que contrariem a definição.

ÍNDICE ALFABÉTICO

BIBLIOGRAFIA

Azevedo, Alberto, *Introdução à teoria dos grupos*, Rio de Janeiro, IMPA, 1969.
Barshay, Jacob, *Topics in Ring Theory*, W. A. Benjamin, Inc., New York, 1969.
Birkhoff, G., *Álgebra Moderna*, Barcelona, Editorial Teide, 1954.
Burton, David M., *A first Course in Rings and Ideals*, Addison-Wesley Publishing Company, Reading, 1968.
Carmichael, Robert D., *Introduction to the Theory of Groups of Finite Order*, Dorer, 1956.
Dean, R. A., *Elements of Abstract Algebra*, Wiley International Edition, New York, 1967.
Deskins, W. E., *Abstract Algebra*, The Macmillan Company, New York, 1964.
Gentile, Enzo R., *Estructuras algebraicas (1)*, Washington, OEA, 1971.
Godement, Roger, *Cours d'Algèbre*, Hermann, Paris, 1963.
Gomes, Alvercio M., *Introdução à Álgebra Moderna*, Rio de Janeiro, FNF, 1960.
Gray, Mary, *A Radical Approach to Algebra*, Addison - Wesley Publishing Company, Reading, 1970.
Jones, Burton W., *An introduction to modern algebra*, New York, Macmillan Publishing, 1975.
Lang, Serge, *Estruturas algébricas*, Rio de Janeiro, Ao Livro Técnico, 1972.
Mac Dufee, C. C., *An Introduction to Abstract Algebra*, N.Y., John Wiley, 1961.
MaCoy, Neal H., *Rings and Ideals*, The Carus Mathematical Monograph, 1948.
Monteiro, L. H. Jacy, *Elementos de Álgebra*, IMPA, Rio de Janeiro, 1971.
Pinto, Herbert F., *Problemas e exercícios de álgebra superior*, Rio de Janeiro, Editora Científica, 1962.
Rotmann, Joseph J., *The Theory of Groups*, An Introduction, Allyn and Bacon, Inc., New York, 1971.
Vilanova, Clóvis, *Elementos da teoria dos grupos e da teoria dos anéis*, 1972
Waerden, B. L. Van der, *Modern Algebra*, N. Y., Frederick Ungar, 1949.