UNIVERSIDADE DO ESTADO DO PARÁ
DEPARTAMENTO DE MATEMÁTICA, ESTATÍSTICA E INFORMÁTICA
LICENCIATURA EM MATEMÁTICA

CCSE

CENTRO DE CIÊNCIAS SOCIAIS E EDUCAÇÃO

ALGEBRA

Pedro Franco de Sá
Miguel Chaquian

Marília Brasil Xavier
REITORA

Prof. Rubens Vilhena Fonseca
COORDENADOR GERAL DOS CURSOS DE MATEMÁTICA

UEPA
UNIVERSIDADE DO ESTADO DO PARÁ

MATERIAL DIDÁTICO

EDITORAÇÃO ELETRONICA

Odivaldo Teixeira Lopes

ARTE FINAL DA CAPA

Odivaldo Teixeira Lopes

REALIZAÇÃO

UEPA
UNIVERSIDADE DO ESTADO DO PARÁ

Belém - Pará - Brasil
- 2011 -

SUMÁRIO

Disciplina: ÁLGEBRA

I – IDENTIFICAÇÃO:

DISCIPLINA: **ÁLGEBRA**

CARGA HORÁRIA TOTAL: 120 h/a

II – OBJETIVO GERAl DA DISCIPLINA:

Introduzir os conceitos fundamentais da álgebra, apresentando uma construção lógico-formal das estruturas algébrica de modo que possa prover o estudante com uma base que lhe permita a ampliação de seus conhecimentos matemáticos em diversas direções.

III – CONTEÚDO PROGRAMÁTICO:

Unidade I – Relações
1.1. Relações binárias e suas propriedades
1.2. Relações de equivalência
1.3. Relações de ordem
1.4. Limites superiores e inferiores, supremo e ínfimo, máximo e mínimo, maximal e minimal.

Unidade II – Grupos e Subgrupos
2.1. Leis de composição interna e suas propriedades
2.2. Tábua de uma operação
2.3. Grupóide, semigrupo, monóide, grupo, grupo comutativo.
2.4. Propriedades de grupo
2.5. Subgrupos

Unidade III – Homomorfismo de Grupos
3.1. Homomorfismo e classificação do homomorfismo.
3.2. Propriedades dos Homomorfismos
3.3. Núcleo de um Homomorfismo.
3.4. Homomorfismos Especiais

Unidade IV – Classes Laterais
4.1. Classe Lateral à Direita
4.2. Classe Lateral à Esquerda
4.3. Propriedades das Classes Laterais
4.4. Subgrupo Normal

Unidade V – Anéis e Corpos
5.1. Anel
5.2. Anéis comutativos, anéis com unidade e anéis de integridade,
5.4 Subanéis.
5.5 Corpo.

INTRODUÇÃO

O século dezenove, mais do que qualquer período precedente, mereceu ser conhecido como Idade Áurea da matemática. O que se acrescentou ao assunto durante esses cem anos supera de longe, tanto em quantidade quanto em qualidade , a produtividade total combinada de todas as épocas precedentes.

Em 1892 um novo mundo na geometria foi descoberto por Lobachevsky, um russo que tivera um professor alemão, e em 1874 o campo da análise fora assombrado pela matemática do infinito introduzido por Cantor, um alemão nascido na Rússia. A França já não era mais o centro reconhecido do mundo matemático, embora fornecesse a carreira meteórica de Évariste Galois (1811 – 1832). O caráter internacional do assunto se percebe no fato de as duas contribuições mais revolucionárias na álgebra terem sido feitas, em 1843 e 1847, por matemáticos que ensinavam na Irlanda, embora, os contribuidores mais prolíficos à álgebra do século dezenove tenham sido os ingleses que passaram algum tempo na América, - Arthur Caley (1821 – 1895) e J. J. Sylvester (1814 – 1897) – e foi principalmente na universidade de onde esses provinham, Camdridge, que se deu o aparecimento da álgebra moderna.

O ponto de virada na matemática inglesa veio em 1815, o algebrista George Peacock (1791 – 1858) não produziu resultados novos notáveis em matemática, mas teve grande importância na reforma do assunto na Inglaterra, especialmente no que diz respeito à álgebra. Num esforço para justificar as idéias mais amplas na álgebra, Peacock em 1830 publicou seu *Treatise on Algebra*, em que procurou dar à álgebra uma estrutura lógica comparável à de *Os elementos* de Euclides. A álgebra de Peacock tinha sugerido que os símbolos para objetos na álgebra não precisam indicar números, e Augustus De Morgan (1806 – 1971) argüía que as interpretações dos símbolos para as operações eram também arbitrárias; George Boole (1815 – 1864) levou o formalismo à sua conclusão. A matemática já não estava limitada a questões de número e grandeza contínua. Aqui pela primeira vez está claramente expressa a idéia de que a característica essencial da matemática é não tanto seu conteúdo quanto sua forma. Se qualquer tópico é apresentado de tal modo que consiste de símbolos e regras precisas de operação sobre símbolos, sujeitas apenas à exigência de consistência interna, tal tópico é parte da matemática.

A multiplicidade de álgebra inventadas no século dezenove poderia ter dado à matemática uma tendência centrífuga se não tivessem sido desenvolvidas certos conceitos estruturais. Um dois mais importantes desses foi a noção de grupo, cujo papel unificador na geometria já foi indicado. Na álgebra o conceito de grupo foi sem dúvida a força mais importante par a coesão , e foi um fator essencial no surgimento das idéias abstratas. Não houve uma pessoa responsável pelo surgimento da idéia grupo, mas a figura que mais se sobressai neste contexto foi o homem que deu o nome a esse conceito, o jovem Évariste Galois, morto tragicamente antes de completar vinte anos. A obra de Galois foi importante não só por tornar a noção abstrata de grupo fundamental na teoria das equações, mas também por levar, através das contribuições de J. W. R. Dedekind (1831 – 1916), Leopold Kronecker (1823 – 1891) e Ernst Eduard Kummer (1810 – 1893), ao que se pode chamar tratamento aritmético da álgebra, algo parecido com a aritmetização da análise, isto significa o desenvolvimento de um cuidadoso tratamento postulacional da estrutura algébrica em termos de vários corpos de números.

A Itália tinha parte um tanto menos ativa no desenvolvimento da álgebra que a França, a Alemanha e a Inglaterra, mas durante os últimos anos do século dezenove houve matemáticos italianos que se interessaram profundamente pela lógica matemática. O mais conhecido desses foi Giuseppe Peano (1858 – 1932) cujo nome é lembrado hoje em conexão com os axiomas de Peano dos quais dependem tantas construções rigorosas da álgebra e da análise.

O alto grau de abstração formal que se introduziu na análise, geometria e topologia no começo do século vinte não podia deixar de invadir a álgebra. O resultado de um novo tipo de álgebra, às vezes inadequadamente descrito como "álgebra moderna", produto em grande parte do segundo terço do século. É de fato verdade que um processo gradual de generalização na álgebra tinha sido desenvolvido no século dezenove, mas no século vinte o grau de abstração deu uma virada brusca, pois x e y já não representavam mais necessariamente números desconhecidos (reais ou complexos) ou segmentos, como na obra de Descartes; agora podiam designar elementos de qualquer tipo – substituições, figuras geométricas, matrizes, polinômios, funções, etc.

A notável expansão da matemática aplicada no século vinte de modo algum diminuiu o ritmo do desenvolvimento da matemática pura, nem o surgimento de novos ramos diminuiu o vigor dos antigo.

Os conceitos fundamentais da álgebra moderna (ou abstrata), topologia e espaços vetoriais foram estabelecidos entre 1920 e 1940, mas a vintena de anos seguinte viu uma verdadeira revolução nos métodos da topologia algébrica que se estendeu à álgebra e à análise, resultando uma nova disciplina chamada álgebra homológica. A álgebra homológica é um desenvolvimento da álgebra abstrata que trata de resultados válidos para muitas espécies diferentes de espaços – uma invasão do domínio da álgebra pura pela topologia algébrica. Nunca antes a matemática esteve tão unificada quanto hoje, pois os resultados desse ramo têm aplicação tão ampla que as etiquetas antigas, álgebra, , análise, geometria, já não se ajustam aos resultados de pesquisas recentes.

A maior parte do enorme desenvolvimento durante os vinte anos seguintes à Segunda Grande Guerra Mundial teve pouco que ver com as ciências naturais, sendo estimulada por problemas dentro da própria matemática pura; no entanto durante o mesmo período as aplicações da matemática à ciência se multiplicaram incrivelmente. A explicação dessa anomalia parece clara : a abstração e percepção de estruturas tem tido papel cada vez mais importante no estudo da natureza, como na matemática. Por isso mesmo em nossos dias de pensamento superabstrato, a matemática continua a ser a linguagem da ciência, tal como era na antigüidade. No entanto, loucura e sabedoria estão tão misturadas na sociedade humana que há agora uma possibilidade muito real de que a matemática do homem se torne um dia o instrumento de sua própria destruição.

UNIDADE I - RELAÇÕES

1.1. RELAÇÕES BINÁRIAS E SUAS PROPRIEDADES

PRODUTO CARTESIANO

Definição:

Sejam **A** e **B** dois conjuntos não vazios. Chama-se ***produto cartesiano*** de **A** por **B** o conjunto formado por todos os pares ordenados **(*x* , *y*)** tais que o primeiro elemento ***x*** pertence ao conjunto **A** e o segundo elemento ***y*** pertence ao conjunto **B** .

Este conjunto produto representa-se por **AxB**, que se lê **"A por B"** , **"A vezes B"** ou **"A cartesiano B"**. Simbolicamente, temos:

$$A \times B = \{ (x , y) \mid x \in A \ \ e \ \ y \in B \}$$

Se $B \neq A$, como $B \times A = \{ (y , x) \mid y \in B \ \ e \ \ x \in A \}$ e $(x , y) \neq (y , x)$, segue-se que $A \times B \neq B \times A$, isto é, o produto cartesiano de dois conjuntos não goza da propriedade comutativa.

Se os conjuntos **A** e **B** são finitos e têm respectivamente **p** e **q** elementos, então o produto cartesiano **AxB** também é um conjunto finito e tem **p.q** elementos, isto é, o número de **AxB** é igual ao produto do número de elementos de **A** pelo número de elementos de **B** :

$$n(A \times B) = n(A).n(B)$$

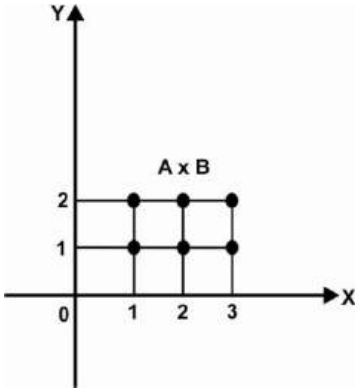
Exemplos:

01. Sejam os conjuntos: A = {1, 2, 3} e B = { 1, 2}. Temos:

AxB = {(1,1); (1,2); (2,1); (2,2); (3,1); (3,2)} e BxA = {(1,1); (1,2); (1,3); (2,1); (2,2); (2,3)}

O produto cartesiano de dois conjuntos pode ser representado por um ***diagrama cartesiano***, por uma ***tabela de dupla*** entrada ou por um ***diagrama sagital***.

Diagrama Cartesiano



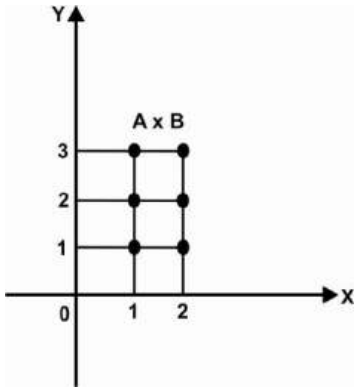
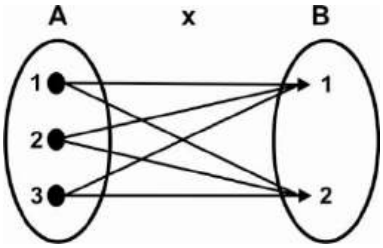


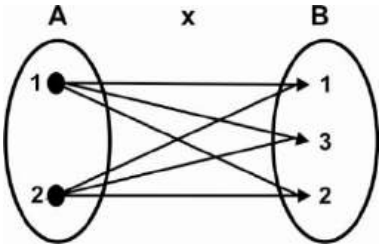
Tabela de Dupla Entrada

A x B	1	2
1	(1,1)	(1,2)
2	(2,1)	(2,2)
3	(3,1)	(3,2)

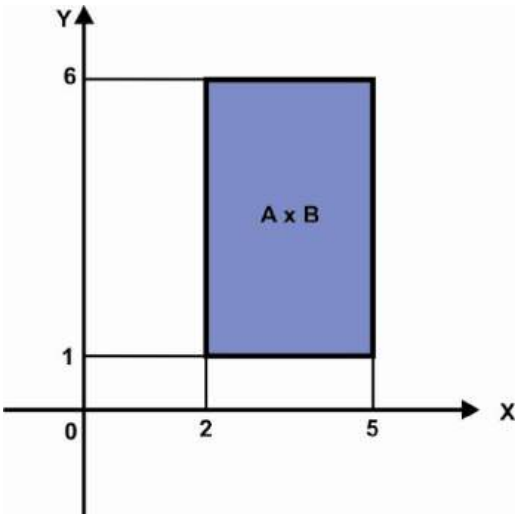
B x A	1	2	3
1	(1,1)	(1,2)	(1,3)
2	(2,1)	(2,2)	(2,3)

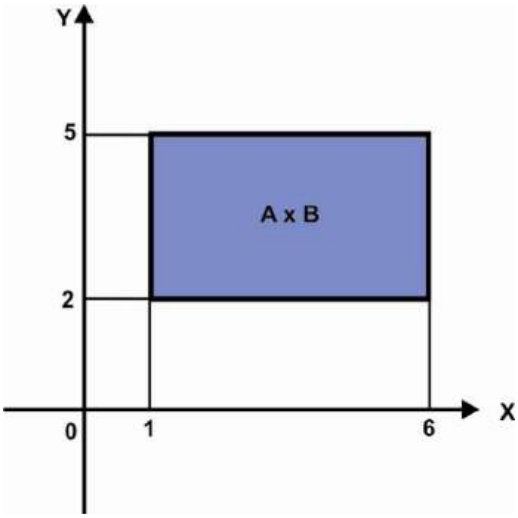
Diagrama Sagital





02. Sejam os conjuntos : $A = \{x \in \Re \mid 2 \leq x \leq 5\}$ e $B = \{ y \in \Re \mid 1 \leq y \leq 6 \}$. Temos:





RELAÇÃO

Definição:

Sejam **A** e **B** dois conjuntos não vazios. Chama-se de ***relação binária de* A *em* B** ou apenas ***relação de* A *em* B** todo subconjunto **R** de **A x B** , isto é :

$$\text{R é relação de A em B} \Leftrightarrow R \subset A \times B$$

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 está relacionado com b segundo R"**). Se $(a,b) \notin R$, escrevemos **a R/b**

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

Exemplos:

01. Sejam os conjuntos A = { 1, 2, 3, 4 } e B = { 1, 3, 5, 7, 9 }. Qualquer subconjunto de A x B é uma relação de A em B, assim, as relações abaixo são relações de A em B :

a) $R_1 = \{(1,1); (1,3); (1,5); (1,7); (1,9)\}$

b) $R_2 = \{(1,1); (2,3); (3,5); (4,7)\}$

c) $R_3 = \{(2,1); (1,3)\}$

d) $R_4 = AxB$

e) $R_5 = \varnothing$

f) $R_6 = \{(x,y) \in AxB \mid x + 5 < y\} = \{(1,7); (1,9); (2,9); (3;9)\}$

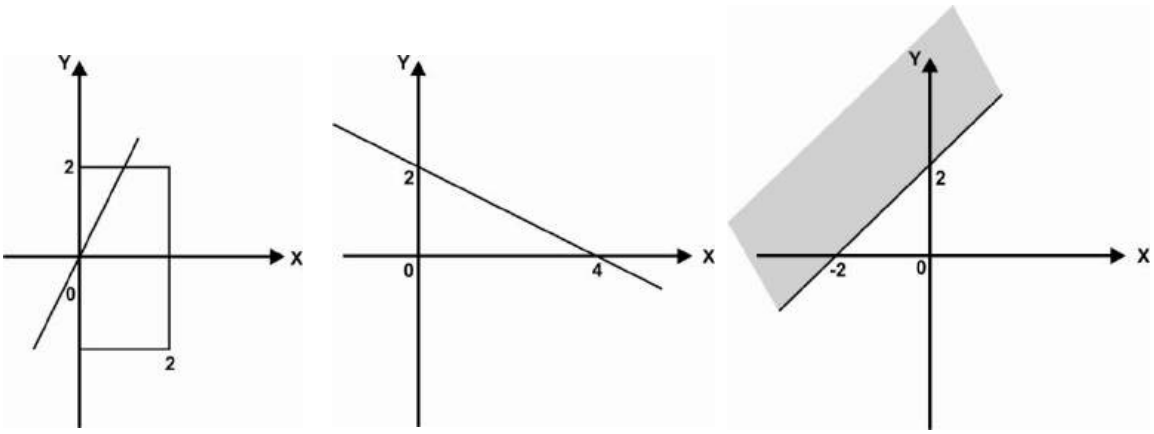
02. Dados os conjuntos A = $\Re$ e B = $\Re$. As relações abaixo são relações de A em B :

a) $R_7 = \{(x,y) \in \Re^2 \mid x = y\}$

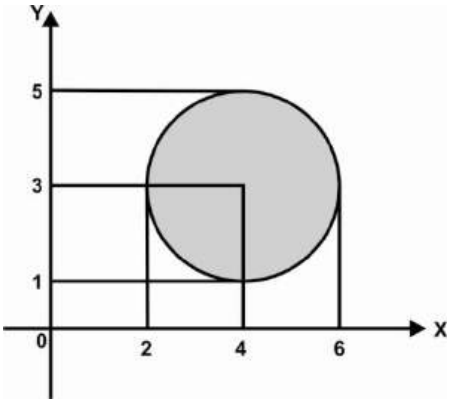
b) $R_8 = \{(x,y) \in \Re^2 \mid 2x + 4y - 8 = 0\}$

c) $R_9 = \{(x,y) \in \Re^2 \mid x - y + 2 < 0\}$

e possuem as respectivas representações:



03. A relação $R_{10} = \{(x,y) \in \Re^2 \mid (x-4)^2 + (y-3)^2 < 4\}$ possui a seguinte representação :



DOMÍNIO E IMAGEM DE UMA RELAÇÃO

Definição:

Seja **R** uma relação de **A** em **B**.

Chama-se de ***domínio*** de **R** o subconjunto de **A** constituído pelos elementos ***x*** para cada um dos quais existe algum *y* em **B** tal que $(x,y) \in \mathbf{R}$ e denota-se por **D(R)**.

$$\mathbf{D(R) = \{\, x \in A \mid \exists\, y \in B\ ;\ (x,y) \in R\}}$$

Chama-se de ***imagem*** de **R** o subconjunto de **B** constituído pelos elementos ***y*** para cada um dos quais existe algum ***x*** em **A** tal que $(x,y) \in \mathbf{R}$ e denota-se por **Im(R)**.

$$\mathbf{Im(R) = \{\, y \in B \mid \exists\, x \in A\ ;\ (x,y) \in R\}}$$

Em outras palavras, **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** .

Exemplos:

01. Aproveitando os exemplos anteriores de relação, temos que :

a) $D(R_1) = \{ 1 \}$ e $Im(R_1) = B$

b) $D(R_2) = A$ e $Im(R_2) = \{1, 3, 5, 7\}$

c) $D(R_5) = \varnothing$ e $Im(R_1) = \varnothing$

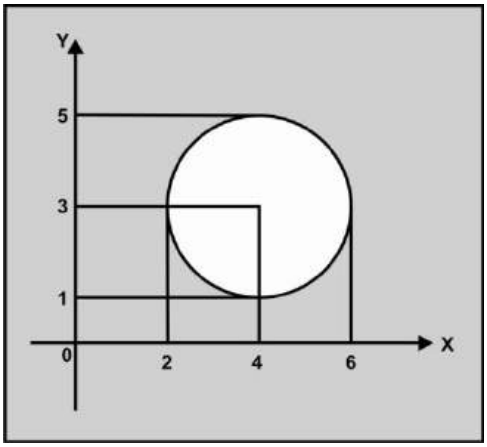
d) $D(R_6) = \{1, 2, 3 \}$ e $Im(R_6) = \{7, 9\}$

e) $D(R_8) = \Re$ e $Im(R_8) = \Re$

f) $D(R_{10}) =]2 , 6[$ e $Im(R_{10}) =]1 , 5[$

- Deixamos ao aluno justificar os domínios e imagens acima determinados.

02. A relação $R_{10} = \{(x,y) \in \Re^2 \mid (x-4)^2 + (y-3)^2 > 4 \}$ possui a seguinte representação:



Observando sua representação temos que: $D(R) = \Re$ e $Im(R) = \Re$.

INVERSA DE UMA RELAÇÃO

Definição:

Seja **R** uma relação de **A** em **B**. Chama-se de relação inversa de **R**, denota-se por $\mathbf{R^{-1}}$, a seguinte relação definida de **B** em **A** :

$$\mathbf{R^{-1} = \{ (y,x) \in B \times A \mid (x,y) \in R \}}$$

A ***relação inversa*** e também denominada de ***relação recíproca***.

No caso particular em que **A = B**, também se diz que $\mathbf{R^{-1}}$ é a ***relação oposta*** de **R** .

Exemplos :

01. Aproveitando os exemplos anteriores de relação, temos que :

a) $R_1^{-1} = \{(1,1); (3,1); (5,1); (7,1); (9,1)\}$

b) $R_2^{-1} = \{(1,1); (3,2); (5,3); (7,4)\}$

c) $R_3^{-1} = \{(1,2); (3,1)\}$

d) $R_4^{-1} = BxA$

e) $R_5^{-1} = \varnothing$

f) $R_6^{-1} = \{(x,y) \in BxA \mid y + 5 < x \} = \{(y,x) \in BxA \mid x + 5 < y \}$

g) $R_7^{-1} = \{(x,y) \in \Re^2 \mid x = y \}$

h) $R_8^{-1} = \{(x,y) \in \Re^2 \mid 2y + 4x - 8 = 0 \}$

i) $R_9^{-1} = \{(x,y) \in \Re^2 \mid y - x + 2 < 0 \}$

j) $R_{10}^{-1} = \{(x,y) \in \Re^2 \mid (y-4)^2 + (x-3)^2 < 4 \}$

Sugerimos ao aluno que represente as relações inversas no plano cartesiano e faça uma analogia com a respctivarelação definida anteriormente.

Qual a conclusão que podemos tirar quando representamos a relação R e sua inversa R^{-1} ?

RELAÇÃO SOBRE UM CONJUNTO

Definição:

Seja **R** uma relação definida de **A** em **A**. Neste caso diz-se que a relação **R *é uma relação sobre*** A ou que **R *é uma relação em*** **A** .

As relações R_7 , R_8 , R_9 e R_{10} são exemplos de relações sobre o conjunto $A = \Re$.

Propriedades

Seja **R** uma relação em **A**. Então podemos verificar as seguintes propriedades:

REFLEXIVA

Diz-se que **R** é ***reflexiva*** quando a condição abaixo está satisfeita :

($\forall$ ***x*** $\in$ **A** ; tem-se ***x*****R*****x***)

SIMÉTRICA

Diz-se que a **R** é ***simétrica*** quando a condição abaixo está satisfeita :

$(\forall \boldsymbol{x}, \boldsymbol{y} \in \mathbf{A}; \boldsymbol{x}\mathbf{R}\boldsymbol{y} \Rightarrow \boldsymbol{y}\mathbf{R}\boldsymbol{x})$

TRANSITIVA

Diz-se que **R** é transitiva quando a condição abaixo está satisfeita :

$(\forall \boldsymbol{x}, \boldsymbol{y} \text{ e } \boldsymbol{z} \in \mathbf{A}; \boldsymbol{x}\mathbf{R}\boldsymbol{y} \text{ e } \boldsymbol{y}\mathbf{R}\boldsymbol{z} \Rightarrow \boldsymbol{x}\mathbf{R}\boldsymbol{z})$

ANTI-SIMÉTRICA

Diz que R e anti-simétrica quando a condição abaixo está satisfeita :

$(\forall \boldsymbol{x}, \boldsymbol{y} \in \mathbf{A}; \boldsymbol{x}\mathbf{R}\boldsymbol{y} \text{ e } \boldsymbol{y}\mathbf{R}\boldsymbol{x} \Rightarrow \boldsymbol{x} = \boldsymbol{y})$

Exemplos:

01. Seja A = {1, 2, 3, 4}. Então podemos classificar as relações abaixo em :
    a) R_1 = {(1,1); (1,2); (2,1); (2,2)} Simétrica e Trantsitiva
    b) R_2 = {(1,1); (2,2); (3,3); (4,4)} Reflexiva, Simétrica, Transitiva e Anti-simétrica
    c) R_3 = {(1,2); (2,3); (1,3)} Anti-simétrica e Transitiva
    d) R_5 = AxA Reflexiva, Simétrica e Transitiva
    e) $R_5 = \varnothing$ Simétrica, Transitiva e Anti-simétrica

02. A relação R definida por $\boldsymbol{x}\mathbf{R}\boldsymbol{y} \Leftrightarrow \boldsymbol{x} \leq \boldsymbol{y}$, sobre o conjunto dos números reais é uma relação reflexiva, anti-simétrica e transitiva.

03. A relação R definida por $\boldsymbol{x}\mathbf{R}\boldsymbol{y} \Leftrightarrow \boldsymbol{x} \mid \boldsymbol{y}$ ($\boldsymbol{x}$ divide $\boldsymbol{y}$) ,sobre o conjunto dos inteiros positivos e uma relação reflexiva, anti-simétrica e transitiva.

04. Sendo A o conjunto das retas do espaço, a relação R definida por $\boldsymbol{x}\mathbf{R}\boldsymbol{y} \Leftrightarrow \boldsymbol{x} \parallel \boldsymbol{y}$,é uma relação reflexiva, simétrica e transitiva.

05. A relação $R = \{(x,y) \in \Re^2 \mid (x-4)^2 + (y-4)^2 \geq 4\}$ é uma relação apenas simétrica.

1.2. RELAÇÃO DE EQUIVALÊNCIA

Definição:

Seja **R** uma relação sobre o conjunto **A**. Diz-se que **R** é uma ***relação de equivalência*** em **A**, se for reflexiva, simétrica e transitiva simultaneamente.

1.3. RELAÇÃO DE ORDEM

Definição:

Seja **R** uma relação sobre o conjunto **A**. Diz-se que **R** é uma ***relação de ordem*** em **A**, se for reflexiva, anti-simétrica e transitiva simultaneamente.

Exemplos:

01. Sendo A o conjunto das retas do espaço, a relação R definida por $x\mathbf{R}y \Leftrightarrow x \,//\, y$,é uma relação de equivalência.
02. A relação R definida por $x\mathbf{R}y \Leftrightarrow x \leq y$, sobre o conjunto dos números reais é uma relação de ordem.
03. A relação R definida por $x\mathbf{R}y \Leftrightarrow x \,|\, y$ (x divide y) ,sobre o conjunto dos inteiros positivos e uma relação de ordem.
04. A relação R definida por $x\mathbf{R}y \Leftrightarrow x - y = 3\mathbf{k}$ (onde **k** é um inteiro), sobre o conjunto dos inteiros positivos e uma relação de equivalência.

Observação : Se **R** é uma **relação de ordem em A** e todos os elementos de **A** estão relacionados, então diz-se que **R** é uma **relação de ordem total**, caso contrário, diz-se que **R** é uma **relação de ordem parcial**.

CLASSES DE EQUIVALÊNCIA

Definição:

Sejam **R** uma relação sobre o conjunto **A** e o elemento $\mathbf{a} \in \mathbf{A}$. Chama-se de ***classe de equivalência*** determinada por **a**, módulo **R**, o subconjunto de **A**, definido por :

$$\bar{\mathbf{a}} = \{ x \in \mathbf{A} \mid x\mathbf{R}a \} \quad \text{ou} \quad \bar{\mathbf{a}} = \{ x \in \mathbf{A} \mid a\mathbf{R}x \}$$

CONJUNTO QUOCIENTE

Definição:

Sejam **R** uma relação de equivalência sobre o conjunto **A.** O conjunto formado por todas as classes de equivalência gerada pelos elementos de A é denominado de ***conjunto quociente*** e denotado por **A/R**.

Exemplos

01. As relações abaixo definidas são relações de equivalência em A = {1, 2, 3, 4}:
    a) R_1 = {(1,1); (1,2); (2,1); (2,2); (3,3); (4,4)}

    $\bar{\mathbf{1}}$ = {1, 2} ; $\bar{\mathbf{2}}$ = {1, 2} ; $\bar{\mathbf{3}}$ = {3} e $\bar{\mathbf{4}}$ = {4}

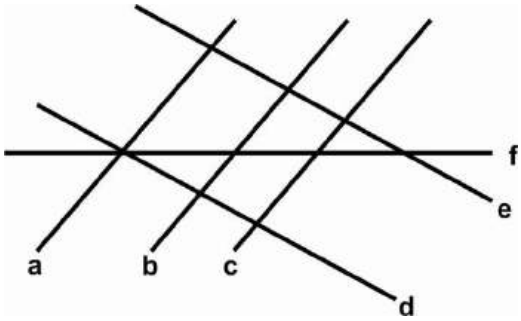
    A/R = { (1, 2}; {3}; {4} }

b) R_2 = {(1,1); (1,2); (2,1); (2,2); (3,3); (3,4); (4,3); (4,4)}

$\bar{\mathbf{1}} = \bar{\mathbf{2}} = \{1, 2\}$; $\bar{\mathbf{3}} = \bar{\mathbf{4}} = \{3, 4\}$

A/R = { (1, 2}; {3,4}}

02. Seja A = {a, b, c, d, e, f} o conjunto das retas da figura abaixo :



Para relação de equivalência **R** definida por $x\mathbf{R}y \Leftrightarrow x \,//\, y$, em A, as classes de equivalência e o conjunto quociente são :

$\bar{\mathbf{a}} = \{a, b, c\} = \bar{\mathbf{b}} = \bar{\mathbf{c}}$

$\bar{\mathbf{d}} = \{d, e\} = \bar{\mathbf{e}}$

$\bar{\mathbf{f}} = \{f\}$

A/R = { {a, b, c}; {d, e}; {f } }

- Deixamos ao encargo do aluno a demnstração do seguinte teorema :

Teorema

Sejam **R** uma relação de equivalência sobre A e os elementos **a**, **b** $\in$ **A**. As seguintes proposições são equivalentes :

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

isto é,

$$\begin{array}{ccc} aRb & \Rightarrow & a \in \bar{a} \\ \Uparrow & & \Downarrow \\ \bar{a} = \bar{b} & \Leftarrow & b \in \bar{a} \end{array}$$

Antes de apresentarmos algumas definições envolvendo relação de ordem é importante sabermos construir um diagrama simplificado e que, sendo **R** uma relação de ordem em **A** e $x\mathbf{R}y$, vale:

$x\mathbf{R}y$ ou x **está relacionado** y ou $x \rightarrow y$ ou x **precede** y ou y **é precedido por** x

DIAGRAMA SIMPLIFICADO

A partir de um exemplo, mostraremos como construir um diagrama simplificado de uma relação de ordem.

Exemplo:

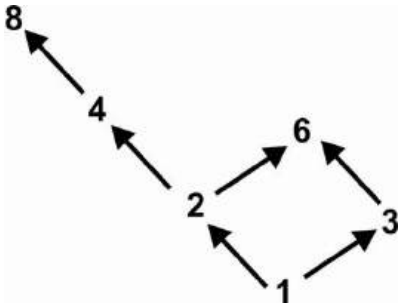
A relação **R** definida por $xRy \Leftrightarrow x \mid y$ (*x* divide *y*), sobre o conjunto **A = {1, 2, 3, 4, 6, 8}** é uma relação de ordem, isto é, **R = {(1,1); (1,2); (1,3); (1,4); (1,6); (1,8); (2,2); (2,4); (2,6); (2,8); (3,3); (3,6); (4,4); (4,8); (6,6); (8,8)}**.

Para fazermos o diagrama simplificado vale as seguintes regras para construção do diagrama:

* Se **(1,2) ∈ R**, então **1 → 2**;

* Se **(1,2)**, **(2,4)** e **(2,4) ∈ R**, então **1 → 2 → 4**, isto é, não há necessidade de indicar **1 → 4**;

* Considerando que toda relação de ordem é uma relação reflexiva, fica subtendido a existência de um laço em torno de todo par **(x,x) ∈ R**;



- Deixamos ao aluno apresentar outras relações de ordem com seus respectivos diagramas simplificados.

Definições:

Seja **R** uma relação de ordem em **A** e **B** um subconjunto de **A**.

Diz–se que $L \in A$ é um ***limite superior*** de **B** quando todo $x \in B$ precede ***L***.

Diz–se que $l \in A$ é um ***limite inferior*** de **B** quando todo $x \in B$ é precedido por ***l***.

Chama–se de ***supremo*** do conjunto **B** ao "menor" dos limites superiores, caso exista.

Chama–se de ***ínfimo*** do conjunto **B** ao "maior" dos limites inferiores, caso exista.

Um elemento $M \in B$ é um ***máximo*** de **B**, quando ele for um limite superior de **B**.

Um elemento $m \in B$ é um ***mínimo*** de **B**, quando ele for um limite inferior de **B**.

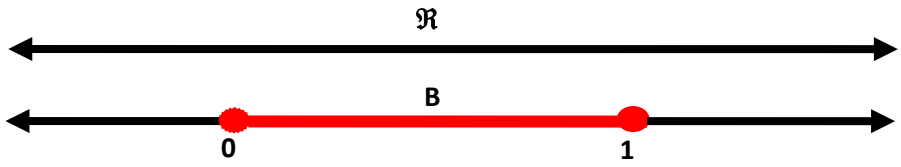
Diz–se que $M_0 \in B$ é ***maximal*** de **B**, se o único elemento de **B** precedido por M_0 é o próprio.

Diz–se que $m_0 \in B$ é ***minimal*** de **B**, se o único elemento de **B** que precede m_0 é o próprio.

Exemplos:

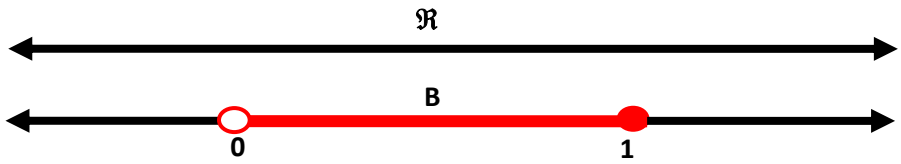
01. Sejam a relação **R** definida por $xRy \Leftrightarrow x \leq y$ sobre o conjunto **A** = $\Re$ e o subconjunto **B = [0 , 1]** de **A**.

02. Representando **A** e **B** em retas, temos:



Limite(s) superior(es) do sub conjunto B:	Lim sup(B)	=	$\{ L \in \Re \mid L \geq 1\}$
Limite(s) inferior(es) do sbconmjunto B:	Lim inf(B)	=	$\{ l \in \Re \mid l \leq 0 \}$
Supremo do subconjunto B:	Sup(B)	=	1
Ínfimo do sbconjunto B:	Ínf(B)	=	0
Máximo do subconjunto B:	Máx(B)	=	1
Mínimo do sbconjunto B:	Mín(B)	=	0
Maximal do subconjunto B:	Maximal(B)	=	1
Minimal do sbconjunto B:	Minimal(B)	=	0

03. Sejam a relação **R** definida por $xRy \Leftrightarrow x \leq y$ sobre o conjunto **A** = $\Re$ e o subconjunto **B =] 0 , 1]** de **A**.
Representando **A** e **B** em retas, temos:

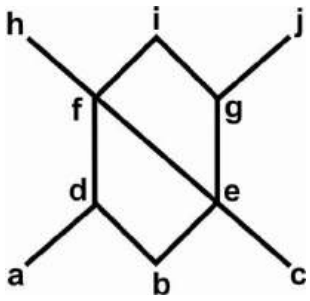


Limite(s) superior(es) do sub conjunto B:	Lim sup(B)	=	$\{ L \in \Re \mid L \geq 1\}$
Limite(s) inferior(es) do sbconmjunto B:	Lim inf(B)	=	$\{ l \in \Re \mid l \leq 0 \}$
Supremo do subconjunto B:	Sup(B)	=	1
Ínfimo do sbconjunto B:	Ínf(B)	=	0
Máximo do subconjunto B:	Máx(B)	=	1
Mínimo do sbconjunto B:	Mín(B)	=	Não existe.
Maximal do subconjunto B:	Maximal(B)	=	1
Minimal do sbconjunto B:	Minimal(B)	=	Não existe.

04. Abaixo 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 supremo, o ínfimo, o máximo e o mínimo de A = {d, e}.

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



UNIDADE II - GRUPOS E SUBGRUPOS

2.1. LEI DE COMPOSIÇÃO INTERNA E SUAS PROPRIEDADES

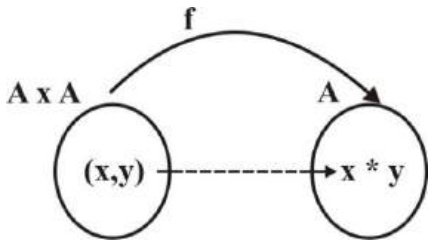
Definição:

Chama-se ***operação interna em*** **A** ou apenas ***operação em*** **A**, toda aplicação **f: AxA** $\rightarrow$ **A** do produto cartesiano **AxA** em **A** .

Portanto, uma operação **f** em A faz corresponder a todo par ordenado **(*x*,*y*)** de **AxA** um único elemento **f[(*x*,*y*)] = *x* ∗ *y*** (lê-se : "***x* estrela *y***") de A. Neste caso, diremos também que **A** é um conjunto munido da operação ∗ .

O elemento ***x* ∗ *y*** é denominado de ***composto*** de ***x*** e ***y*** pela operação **f**; os elementos ***x*** e ***y*** do composto ***x* ∗ *y*** são denominados de ***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***.

Simbolicamente:



Diz-se que o conjunto **A** acha-se munido da operação $*$, o conjunto **AxA** chama-se domínio da operação e denota-se por **(A , $*$)** .

Outros símbolos poderão ser utilizados para operação genérica como: $\otimes$, $\oplus$, $\perp$, o e $\square$.

Exemplos e Contra-exemplos:

01. A adição e a multiplicação de números naturais são operações internas no conjunto dos números naturais, porque :

$$(x,y) \in NxN \rightarrow x + y \in N \text{ e } (x,y) \in NxN \rightarrow x.y \in N$$

02. A divisão de racionais não nulos é uma operação interna no conjunto dos números racionais não nulos, porque:

$$(x,y) \in Q \text{ x } Q \rightarrow \frac{x}{y} \in Q$$

03. Observe que a diferença de números naturais não é uma operação interna em *N*, porém, a mesma operação definida no conjunto dos números inteiros é uma operação interna em *Z*.

04. A adição em $M_{mxn}(\Re)$ é uma operação interna.

05. Justifique porque a operação x^y não é uma operação interna no conjunto dos números racionais.

2.2. TÁBUA DE UMA OPERAÇÃO

Uma operação $*$ num conjunto finito **A** pode ser definida por meio de uma ***tabela de dupla entrada*** que indique o composto $x * y$ correspondente a cada par ordenado **(*x*,*y*)** de elementos de **A**, denominada de ***tábua da operação*** $*$ em **A**.

Exemplos:

01. A operação definida por $x * y$ = **mdc(*x*,*y*)** em A = {1, 2, 3, 4} pode ser representada pela seguinte tábua :

*	1	2	3
1	1	1	1
2	1	2	1
3	1	1	3

02. A operação definida por $x * y = x \cap y$ em A = $\wp(\{1, 2\})$ pode ser representada pela seguinte tábua :

⊗	∅	{ 1 }	{ 2 }	{ 1, 2}
∅	∅	∅	∅	∅
{ 1 }	∅	{ 1 }	∅	{ 1 }
{ 2 }	∅	∅	{ 2 }	{ 2 }
{ 1, 2}	∅	{ 1 }	{ 2 }	{ 1, 2 }

Sugerimos ao leitor que faça a construção da tábua utilizando a operação de reunião.

PROPRIEDADES DE UMA OPERAÇÃO

Seja $*$ uma lei de composição interna em **A**. A operação $*$ pode ter as seguintes propriedades :

IDEMPOTÊNCIA

Diz-se que a operação $*$ em **A** é ***idempotente*** se, e somente se, para todo elemento x de **A** tem-se $x*x = x$.

Observe que as operações representadas anteriormente pelas tábuas são idempotentes.

ASSOCIATIVA

Diz-se que a operação $*$ em **A** é ***associativa*** quando, quaisquer que sejam os elementos x, y e z de **A**, tem-se $x * (y * z) = (x * y) * z$.

É fácil notar que as operações abaixo são associativas nos respectivos conjuntos;

a) As adições e multiplicações em N, Z, Q, R e C .

b) A composição de funções de R em R .

c) A operação $x*y = x + y + 2xy$ no conjuntos dos números inteiros.

COMUTATIVA

Diz-se que a operação $*$ em **A** é ***comutativa*** quando, quaisquer que sejam os elementos x e y de **A**, tem-se $x * y = y * x$.

É fácil ver que as operações abaixo são associativas nos respectivos conjuntos;

a) As adições e multiplicações em N, Z, Q, R e C .

b) A operação $x*y = x + y + 2xy$ no conjuntos dos números inteiros.

EXISTÊNCIA DO ELEMENTO NEUTRO

Diz-se que $e \in A$ é **elemento neutro** para a operação $*$ em **A** se, e somente se, para todo elemento x de **A** tem-se (I) $x * e = x$ e (II) $x * e = x$.

Observe que a condição $x * e = e * x$ sempre ocorre quando a operação é comutativa, neste caso será necessário verificarmos apenas (I) ou (II).

Quando apenas (I) se verifica, diz-se então que e é um ***elemento neutro à direita*** e, quando apenas (II) se verifica, diz-se então que e é um ***elemento neutro à esquerda***. É evidente que se e é elemento neutro à esquerda e a direita para a operação $*$, então dizemos que e é ***elemento neutro*** para esta operação.

É fácil identificar o respectivo elemento neutro de cada operação abaixo nos respectivos conjuntos;

a) O elemento neutro da adição e multiplicação em N, Z, Q, R e C são 0 (zero) e o 1 (um), respectivamente.

b) Para a composição de funções de R em R , o elemento neutro é a função identidade, definida por $f(x) = x$.

Por outro lado a operação $x*y = x + y + xy$ no conjuntos dos números inteiros não admite elemento neutro, de fato:

Utilizaremos apenas (I) devido a operação ser comutativa

$$x * e = x$$

$$x + e + xe = x$$

$$e + xe = 0$$

$$e(1 + x) = 0$$

somente implica em $e = 0$ para $x \neq -1$, portanto, não vale para todos os inteiros.

Deixamos ao encargo do aluno a demonstração da seguinte proposição :

Proposição

Seja $*$ uma operação interna em **A**. Se a operação $*$ admite elemento neutro, então ele é único.

EXISTÊNCIA DO ELEMENTO SIMÉTRICO

Diz-se que $x \in \mathbf{A}$ é **elemento simetrizável** para a operação $*$ em **A**, que possui elemento neutro e, se existir $x' \in \mathbf{A}$ tal que (I) $x * x' = e$ e (II) $x' * x = e$.

Observe que a condição $x * x' = x' * x$ sempre ocorre quando a operação é comutativa, neste caso será necessário verificarmos apenas (I) ou (II).

Quando apenas (I) se verifica, diz-se então que x' é um ***elemento simétrico à direita*** e, quando apenas (II) se verifica, diz-se então que x' é um ***elemento simétrico à esquerda***. É evidente que se x' é elemento simétrico à esquerda e a direita para a operação $*$, então dizemos que x' é ***elemento simétrico de*** x para esta operação.

Quando a operação $*$ é uma adição, o simétrico de x também é chamado de ***oposto de*** x e denotado por $-x$. No caso da operação $*$ ser uma multiplicação, o simétrico de x é denominado de ***inverso de*** x e denotado por x^{-1} .

Apenas os elementos **0** e **– 1** são simetrizáveis no conjunto dos números inteiros para a operação $x*y = x + y + 2xy$, cujo elemento neutro é $e = 0$. De fato:

Utilizaremos apenas (I) devido a operação ser comutativa

$x * x' = e$

$x + x' + 2xx' = 0$

$x' + 2xx' = -x$

$x'(1 + 2x) = -x$

Como não existe inteiro que torne o fator $(1 + 2x)$ nulo, então podemos concluir que:

$$x' = -\frac{x}{1+2x}$$

Os únicos inteiros que substituídos no lugar de x resultam em inteiro são **0** e **– 1**.

Assim, $U_*(Z) = \{ -1, 0 \}$, onde U_* representa o conjunto dos elementos simetrizáveis de Z.

Utilizaremos a notação $\mathbf{U_*(A)}$ para representar o conjunto dos elementos simetrizáveis em **A** para a operação $*$.

Deixamos ao encargo do leitor a demonstração da seguinte proposição:

Proposição

Seja $*$ uma operação interna em **A**, associativa e admite elemento neutro ***e***, então podemos concluir que:

a) Todo elemento $x \in \mathbf{A}$ admite um único simétrico.

b) O simétrico do simétrico, de um elemento $x \in \mathbf{A}$, é o próprio x .

c) Se x e y são elementos simetrizáveis em **A** e seus respectivos simétricos são **x'** e **y'**, então $x * y$ é simetrizável e seu simétrico é $y' * x'$.

ELEMENTO REGULAR

Diz-se que um elemento $a \in \mathbf{A}$ é regular ou simplificável em relação a operação $*$ se, e somente se, quaisquer que sejam os elementos x e y de A, as relações :

(I) $x * a = y * a \Rightarrow x = y$

(II) $a * x = a * y \Rightarrow x = y$

Observe que a condição $x * a = a * x$ e $y * a = a * y$ sempre ocorrem quando a operação é comutativa, neste caso será necessário verificarmos apenas (I) ou (II).

Quando apenas (I) se verifica, diz-se então que a é um ***elemento regular à direita*** e, quando apenas (II) se verifica, diz-se então que x' é um ***elemento regular à esquerda***. É evidente que se a é elemento regular à esquerda e a direita para a operação $*$, então dizemos que a é ***elemento regular*** para esta operação.

Todo número real a é regular para a operação $x*y = x + y$.

Todos os elementos do conjunto $\Re - \{-1/2\}$ são regulares para a operação $x*y = x + y + 2xy$, cujo elemento neutro é $e = 0$. De fato:

Utilizaremos apenas (I) devido a operação ser comutativa

$x * a = y * a$

$x + a + 2xa = y + a + 2ya$

$2xa = 2ya$

$xa = ya$

$x = y$

Assim, $R_*(\Re - \{-1/2\}) = \Re - \{-1/2\}$, onde U_* representa o conjunto dos elementos regulares.

Utilizaremos a notação $\mathbf{R_*(A)}$ para representar o conjunto dos elementos regulares em **A** para a operação $*$.

É notório que um elemento regular $\boldsymbol{a} \in \mathbf{A}$ é regular quando, composto com elementos distintos à esquerda deles ou à direita, gera resultados distintos.

Deixamos ao encargo do leitor a demonstração da seguinte proposição :

Proposição

Se uma operação interna $*$ em **A** é associativa, admite o elemento neutro $\boldsymbol{e}$ e $\boldsymbol{a} \in \mathbf{A}$ é simetrizável, então $\boldsymbol{a}$ é regular.

PARTE FECHADA EM RELAÇÃO A UMA OPERAÇÃO

Definição:

Sejam **G** um conjunto não vazio munido de uma operação $*$ e H um subconjunto não vazio de **G**. Diz-se que **H** é uma parte fechada em relação à operação $*$ em **G**, quando o composto $\boldsymbol{x*y}$ de dois elementos quaisquer $\boldsymbol{x}$ e $\boldsymbol{y}$ de **H**, também for um elemento de **H**.

Exemplo:

01. Sejam $\mathbf{G} = \boldsymbol{C}$, $\mathbf{H} = \{ -\boldsymbol{i}, -1, \boldsymbol{i}, 1\}$ e a operação $\mathbf{Z_1 * Z_2 = Z_1 \,.\, Z_2}$. Observando a tábua abaixo, concluímos que **H** é uma parte fechada de **G**.

$*$	$-i$	-1	i	1
$-i$	-1	i	1	$-i$
-1	i	1	$-i$	-1
i	1	$-i$	-1	i
1	$-i$	-1	i	1

2.3. GRUPÓIDE, SEMIGRUPO, MONÓIDE, GRUPO, GRUPO COMUTATIVO.

GRUPÓIDE

Definição:

Seja **G** um conjunto não vazio, munido de uma operação $*$. Chama-se de ***grupóide*** ao par **(G, $*$)** .

SEMIGRUPO

Definição:

Semigrupo é um par ordenado **(G , $*$)** formado por um conjunto não vazio **G** e uma operação associativa $*$ em **G**, isto é, todo grupóide cuja operação $*$ é associativa.

MONÓIDE

Definição:

Chama-se de ***monóide*** a todo grupóide **(G, $*$)** cuja operação $*$ é associativa e admite elemento neutro, ou todo semi–grupo cuja operação $*$ tem admite elemento neutro.

GRUPO

Definição:

Seja **G** um conjunto não vazio munido de uma operação $*$. Diz–se que a operação $*$ define uma ***estrutura de grupo sobre o conjunto*** **G** ou que o conjunto **G** é um ***grupo*** em relação à operação $*$ quando as seguintes propriedades são válidas:

(G_1) Associativa

– Quaisquer que sejam x, y e $z \in$ **G**, tem–se $x*(y*z) = (x*y)*z$.

(G_2) Elemento Neutro

– Existe em **G** um elemento e tal que $x*e = e*x$ qualquer que seja $x \in$ **G**.

(G_3) Elementos Simetrizáveis

– Para todo x em **G**, existe um elemento x' em G tal que $x*x' = x'*x = e$.

Por outro lado, **G** é um grupo se o par **(G, $*$)** é um monóide que satisfaz a condição suplementar de que todo elemento de **G** é simetrizável para a operação $*$.

GRUPO COMUTATIVO

Definição:

Se **(G, ∗)** é um grupo e a operação ∗ é comutativa, então diz–se que o par **(G, ∗)** é um ***grupo comutativo*** ou ***grupo abeliano*** (homenagem ao matemático norueguês Niels Henrik Abel do século XIX, 1802 – 1829).

Exemplos:

01. O grupóide **(Q , ∗)** é um grupo abeliano, onde $x*y = x + y$. De fato :

(G_1) $\forall x, y, z \in Q$ tem–se $(x + y) + z = x + (y + z)$

(G_2) $\exists\, e = 0 \in Q$, tal que $\forall x \in Q$ tem–se $0 + x = x + 0 = x$

(G_3) $\forall x \in Q$, $\exists - x \in Q$ tal que $x + (-x) = (-x) + x = 0$

(G_4) $\forall x, y \in Q$, temos $x + y = y + x$

02. O grupóide **(Z, ∗)** munido da operação $x*y = x + y - 10$ possui as seguintes propriedades:

Associativa

$$\begin{aligned}(x*y)*z &= (x + y - 10)*z \\ &= (x + y - 10) + z - 10 \\ &= x + (y + z - 10) - 10 \\ &= x*(y + z - 10) \\ &= x*(y*z)\end{aligned}$$

Comutativa

$x*y = x + y - 10 = y + x - 10 = y*x$

Elemento Neutro

$$\begin{aligned} x*e &= x & \qquad e*x &= x \\ x + e - 10 &= x & \qquad e + x - 10 &= x \\ e &= 10 & \qquad e &= 10\end{aligned}$$

Elementos Simetrizáveis

$$\begin{aligned} x*x' &= e & \qquad x'*x &= e \\ x + x' - 10 &= 0 & \qquad x' + x - 10 &= 0 \\ x' &= 20 - x & \qquad x' &= 20 - x\end{aligned}$$

$U_*(Z) = Z$

Portanto, **(Z, ∗)** é um grupo abeliano.

03. Os grupóides **(Z, +)**; **(Q, +)**; **($\mathfrak{R}$, +)**; **(C, +)**; **(Q^*, .)**; **($\mathfrak{R}^*$, .)** e **(C^*, .)** também são exemplos de grupos comutativos.

04. Deixamos ao encargo do leito provar que os grupóides abaixo são grupos abelianos :

a) G = $\mathfrak{R}$ e $x \oplus y = \sqrt[3]{x^3 + y^3}$

b) G = Q e $x \otimes y = x + y + 3$

Notação

Para simplificar, indicaremos pela notação aditiva – **(G, +)** – quando a operação $*$ for a adição usual e pela notação multiplicativa – **(G, .)** – se a operação $*$ for a multiplicação usual. No primeiro caso diz-se que o grupo **(G, +)** é um ***grupo aditivo*** e no segundo, o grupo **(G, .)** é um ***grupo multiplicativo*** .

GRUPOS FINITOS E INFINITOS. ORDEM DE UM GRUPO

Definição:

Se o conjunto **G** é finito, então diz–se que o grupo **(G, $*$)** é um ***grupo finito*** e o número de elementos de **G**, denotado por **o(G)** ou **n(G)**, é a ***ordem do grupo***. Caso contrário, diz–se que o grupo **(G, $*$)** é um **grupo infinito** e que sua ***ordem*** é infinita.

Exemplos :

01. Seja **G = { – *i*, – 1, *i*, 1}** e a operação $\mathbf{Z_1 * Z_2 = Z_1 \,.\, Z_2}$. Observando a tábua abaixo, concluímos que **G** é um grupo finito e que sua ordem é o(G) = 4.

$*$	$-i$	-1	i	1
$-i$	-1	i	1	$-i$
-1	i	1	$-i$	-1
i	1	$-i$	-1	i
1	$-i$	-1	i	1

02. O grupo **(Z, $*$)** munido da operação $\boldsymbol{x * y = x + y - 10}$ é um grupo infinito e sua ordem é infinita.

2.4. PROPRIEDADES DOS GRUPOS

Seja **(G, ∗)** um grupo.

UNICIDADE DO ELEMENTO NEUTRO

Teorema

O elemento neutro do grupo **(G, ∗)** é único.

UNICIDADE DO ELEMENTO SIMÉTRICO

Teorema

Cada elemento ***x*** do grupo **(G, ∗)** admite um único simétrico.

Corolário

Para todo elemento do grupo **(G, ∗)** cujo simétrico é ***x'***, tem–se **(*x*')' = *x***.

Demonstração:

Pela definição de simétrico, temos:

$$(x')' * x' = e \quad \text{e} \quad x' * (x')' = e$$

$$[(x')' * x'] * x = e * x \qquad x * [x' * (x')'] = x * e$$

$$(x')' * [x' * x] = x \qquad [x * x'] * (x')' = x$$

$$(x')' * e = x \qquad e * (x')' = x$$

$$(x')' = x \qquad (x')' = x$$

SIMÉTRICO DE UM COMPOSTO

Teorema

Quaisquer que sejam ***x*** e ***y*** em **G**, tem–se **(*x* ∗ *y*)' = *y*' ∗ *x*'**.

Demonstração:

Aplicando a propriedade associativa, temos:

$(x*y)*(y'*x') = x*(y*y')*x' = x*e*x' = x*x' =$ e

e, de modo análogo :

$(y'*x')*(x*y) = y'*(x'*x)*y = y'*e*y = y'*y = e$

Portanto, o simétrico do composto $x*y$ é $y'*x'$

ELEMENTOS REGULARES

Teorema

Todos os elementos do grupo **G** são regulares.

É importante notar que num grupo valem as regras de simplificação à esquerda e à direita para a operação $*$ do grupo.

EQUAÇÃO NUM GRUPO

Teorema

A solução da equação $\boldsymbol{x*x = x}$ é única, a saber $\boldsymbol{x = e}$.

Demonstração:

De fato, $x*x = x \Rightarrow (x*x)*x' = x*x' \Rightarrow x*(x*x') = e \Rightarrow x*e = e \Rightarrow x = e$

Por outro lado, supondo que $x_0 \in G$ é também solução da equação $x*x = x$, tem–se:

$x_0 = x_0*e = x_0*(x_0*x_0') = (x_0*x_0)*x_0' = x_0*x_0' = e$

Deste modo, o único elemento idempotente num grupo é o elemento neutro.

Teorema

Quaisquer que sejam os elementos **a** e **b** de **G**, as equações $\mathbf{a*x = b}$ e $\boldsymbol{y*a = b}$ admitem solução única em **G** .

Demonstração;

De fato,

$a*x$	=	b		$y*a$	=	b
$a'*(a*x)$	=	$a'*b$		$(y*a)*a'$	=	$b*a'$
$(a'*a)*x$	=	$a'*b$		$y*(a*a')$	=	$b*a'$
$e*x$	=	$a'*b$		$y*e$	=	$b*a'$
x	=	$a'*b$		y	=	$b*a'$

Por outro lado, supondo que x_0 e $y_0 \in G$ são, respectivamente, soluções das equações $a*x = b$ e $y*a = b$, tem–se :

$x_0 = e*x_0$ e $y_0 = y_0*e$

$x_0 = (a'*a)*x_0$ $\qquad$ $y_0 = y_0*(a*a')$

$x_0 = a'*(a*x_0)$ $\qquad$ $y_0 = (y_0*a)*a'$

$x_0 = a'*b$ $\qquad$ $y_0 = b*a'$

Exemplos:

01. A tábua ao lado representa todas as possíveis operações do grupo G = { a, b, c, d, e, f} levando–se em conta que :

a) G é abeliano

b) O neutro é e

c) a∗f = b∗d = e

d) a∗d = b∗c = f

e) a∗c = b∗b = d

f) c∗d = a

∗	a	b	c	d	e	f
a	b	c	d	f	a	e
b	c	d	f	e	b	a
c	d	f	e	a	c	b
d	f	e	a	b	d	c
e	a	b	c	d	e	f
f	e	a	b	c	f	d

02. Para resolvermos a equação a∗b∗c∗x∗b = c, devemos proceder do seguinte modo:

$a'*a*b*c*x*b*b' = a'*c*b'$

$e*b*c*x*e = a'*c*b'$

$b*c*x = a'*c*b'$

$b'*b*c*x = b'*a'*c*b'$

$e*c*x = b'*a'*c*b'$

$c'*c*x = c'*b'*a'*c*b'$

$e*x = c'*b'*a'*c*b'$

$x = c'*b'*a'*c*b'$

Deixamos ao encargo do leitor determinar outra forma de obter a solução, observando o simétrico de um composto.

2.5. SUBGRUPOS

Definição:

Sejam **(G, ∗)** um grupo e **H** uma parte não vazia do conjunto **G**. O par **(H, ∗)** diz–se um ***subgrupo*** do grupo **(G, ∗)**, quando **H** é fechado à operação ∗ do grupo **G** e **(H, ∗)** também é um grupo, isto é, quando as seguintes condições forem satisfeitas:

(S_1) Quaisquer que sejam os elementos ***x*** e ***y*** de **H**, tem–se $x*y \in H$

(S_2) O par **(H, ∗)** também é um grupo.

A associatividade da operação ∗ em **G** garante a associatividade desta operação em **H**, porque **H** é uma parte não vazia de **G** ($H \subset G$).

Todo grupo **(G, ∗)** em que **o(G) ≥ 1**, admite pelo menos dois subgrupos : **({e}, ∗)** e **(G, ∗)**, denominados de ***subgrupos triviais*** ou ***subgrupos impróprios***. Os demais subgrupos de **(G, ∗)**, se existem, são chamados de ***subgrupos próprios*** .

Exemplos:

01. Sobre o grupo multiplicativo dos reais ($\Re$, .), podemos afirmar que :

a) Os subgrupos triviais são : ($\Re$, .) e ({1}, .) ;

b) Os conjuntos $H_1 = \{-1, 1\}$ e $H_2 = \{x \in \Re \mid x > 0\}$ são subgrupos próprios de ($\Re$, .)

02. O grupo de Klein (Felix Klein 1849 – 1925), de ordem 4, K = { a, b, c, e} representado na tábua abaixo :

∗	**e**	**a**	**b**	**c**
e	**e**	a	b	c
a	a	**e**	c	b
b	b	c	**e**	a
c	c	b	a	**e**

Possui os seguintes subgrupos :

a) Subgrupos triviais : ({e}, ∗) e ({a, b, c, e}, ∗ }

b) Subgrupos próprios : ({e, a}, ∗); ({e, b}, ∗) e ({e, c}, ∗)

03. O par (H = { 2^n | n ∈ Z }, .) é um subgrupo do grupo multiplicativo (G = Q_+^*, .) dos racionais positivos.

04. O grupo G = { – i, – 1, i, 1} é um subgrupo do grupo multiplicativo (C^*, .).

05. Consideremos o grupo G = ℜxℜ = $\Re^2$ munido com a operação ∗ definida por (a,b) ∗ (c,d) = (a + c, b + d). O conjunto H = { (x,y) ∈ $\Re^2$ | y = 2x } é um subgrupo de G.

PROPRIEDADES DOS SUBGRUPOS

Sejam o grupo **(G, ∗)** e **H** um subgrupo de **G**.

ELEMENTO NEUTRO

Teorema

O elemento do neutro do grupo coincide com o elemento neutro de cada um dos seus subgrupos.

Demonstração:

Sejam e_G e e_H os respectivos elementos neutros do grupo G e do subgrupo H.

Como H ⊂ G, temos que e_H ∈ G e que $e_H * e_G = e_G * e_H = e_H$.

Por hipótese e_H é o elemento neutro de H, logo $e_H * e_H = e_H$.

Aplicando a propriedade de elementos simplificáveis em $e_H * e_G = e_H * e_H$, obtemos $e_G = e_H$. Portanto, o elemento neutro do grupo é o mesmo elemento neutro de cada um dos seus subgrupos.

SIMÉTRICO DE UM ELEMENTO

Teorema

O simétrico de qualquer elemento do subgrupo coincide com o seu simétrico no grupo.

Demonstração:

Sejam x ∈ H e e o elemento neutro do grupo e do subgrupo.

Consideremos x'_G e x'_H os simétricos de x em relação ao grupo G e ao subgrupo H, respectivamente, assim :

$$x*x'_G = x'_G*x = e \quad \text{e} \quad x*x'_H = x'_H*x = e$$

Como todo elemento de G é regular, concluímos que $x'_G = x'_H$.

CARACTERIZAÇÃO DOS SUBGRUPOS

Teorema

Seja H um subconjunto não vazio do grupo (G, $*$). Então o par (H, $*$) é um subgrupo de G se, e somente se, as duas condições abaixo são satisfeitas :

(S_1) Dados h_1 , $h_2 \in H$, tem–se $h_1 * h_2 \in H$.

(S_2) Dado $h \in H$, tem–se $h' \in H$.

Demonstração:

Supondo que H seja um subgrupo do grupo G, as condições (S_1) e (S_2) são claramente satisfeitas.

Reciprocamente, supondo que as duas condições (S_1) e (S_2) sejam satisfeitas, temos :

a) A operação $*$ é associativa em H, porque a operação $*$ em G é associativa e $H \subset G$;
b) As condições (S_1) e (S_2) garantem que a operação $*$ é fechada em H, assim como, todos os elementos de H são simetrizáveis;
c) Tomando $h \in H$, pela condição (S_2) $h' \in H$ e pela condição (S_1) $h*h' = h'*h \in H$, assim $e \in H$.

Portanto, H é um subgrupo do grupo G.

Exemplos:

01. Mostraremos que o par ($H = \{ 3^n \mid n \in Z \}$, .) é um subgrupo do grupo multiplicativo dos racionais positivos ($G = Q_+^*$, .).
    a) O neutro do grupo é $e = 1$ que pode ser interpretado como $e = 3^0 = 1$, onde $0 \in Z$;
    b) Dados $h_1 = 3^p$ e $h_2 = 3^q$ elementos de H, com p e q inteiros, temos :
        i. $h_1*h_2 = 3^p.3^q = 3^{p+q} \in H$, pois p + q é inteiro
    c) Seja $h = 3^m$, com m inteiro. Assim,

$h*h' = e \Rightarrow 3^m.h' = 1 \Rightarrow h' = 3^{-m} \Rightarrow h' \in H$, pois – m é inteiro.

Portanto, H é um subgrupo de G

02. O conjunto $H = \{ z = \cos(\theta) + i.\text{sen}(\theta) \mid \theta \in Q \}$ é um subgrupo do grupo multiplicativo dos complexos não nulos (C^*, .). De fato :

a) O neutro do grupo é $e = 1$ que pode ser escrito como $e = \cos(0) + i.\text{sen}(0) \in H$;

b) Dados $h_1 = \cos(\theta_1) + i.\text{sen}(\theta_1)$ e $h_2 = \cos(\theta_2) + i.\text{sen}(\theta_2)$ elementos de H, com θ_1 e θ_2 racionais, temos :

$h_1*h_2 = [\cos(\theta_1) + i.\text{sen}(\theta_2)].[\cos(\theta_2) + i.\text{sen}(\theta_2)]$

$h_1*h_2 = [\cos(\theta_1).\cos(\theta_2) - \text{sen}(\theta_1).\text{sen}(\theta_2)] + i.[\cos(\theta_1).\text{sen}(\theta_2) + \text{sen}(\theta_1).\cos(\theta_2)]$

$h_1*h_2 = \cos(\theta_1 + \theta_2) + i.\text{sen}(\theta_1 + \theta_2)$

$h_1*h_2 \in H$, pois $\theta_1 + \theta_2 = \theta \in Q$;

c) Dado $h = \cos(\theta) + i.\text{sen}(\theta) \in H$, com θ racional. Assim,

$h*h' = e \Rightarrow h.h' = 1 \Rightarrow h' = \frac{1}{h} \Rightarrow h' = \cos(\theta) - i.\text{sen}(\theta) \Rightarrow$

$h' = \cos(-\theta) + i.\text{sen}(-\theta)$, como $-\theta$ é racional então

$h' \in H$.

Portanto, H é um subgrupo de $G = C^*$.

03. O conjunto $H = \{ 2.k \mid k \in Z \}$ é um subgrupo do grupo aditivo dos números inteiros (Z, +). De fato :

a) O neutro do grupo é $e = 0$ que pode ser interpretado como $e = 2.0 = 0$, onde $0 \in Z$;

b) Dados $h_1 = 2.k_1$ e $h_2 = 2.k_2$ elementos de H, com k_1 e k_2 inteiros, temos :

$h_1*h_2 = (2.k_1).(2.k_2) = 2.(2.k_1.k_2) \in H$, pois $2.k_1.k_2 = k$ inteiro

c) Seja $h = 2.k$, com k inteiro. Assim,

$h*h' = e \Rightarrow 2.k + h' = 0 \Rightarrow h' = -2.k \Rightarrow h' = 2.(-k) \Rightarrow$

$h' \in H$, pois $-k$ é inteiro.

Portanto, H é um subgrupo de $G = Z$.

04. O conjunto $H = \{ z \in C \mid |z| = 1 \}$ é um subgrupo do grupo multiplicativo dos números complexos não nulos (C^*, .). De fato :

a) O neutro do grupo é $e = 1 \in H$, pois $|e| = 1$;

b) Dados $h_1 = z_1$ e $h_2 = z_2$ elementos de H, com $|z_1| = 1$ e $|z_2| = 1$, temos :

$|h_1 * h_2| = |z_1.z_2| = |z_1|.|z_2| = 1.1 = 1$, logo $h_1 * h_2 \in H$;

c) Seja $h = z$, com $|z| = 1$. Assim,

$h * h' = e \quad \Rightarrow \quad z \,.\, h' = 1 \quad \Rightarrow \quad h' = \bar{z}$

$|h'| = |\bar{z}| = |z| = 1. \quad \Rightarrow \quad h' \in H.$

Portanto, H é um subgrupo de $G = C^*$.

05. O conjunto $H = \{ x \in Q \mid x > 0\}$ é um subgrupo do grupo multiplicativo dos números racionais não nulos (Q^*, .). De fato :

a) O neutro do grupo é $e = 1 \in H$, pois $e = 1 > 0$;

b) Dados h_1 e h_2 elementos de H, com $h_1 > 0$ e $h_2 > 0$, temos :

$h_1 * h_2 = h_1.h_2 > 0$, logo $h_1 * h_2 \in H$;

c) Seja h elemento de H , com $h > 0$. Assim,

$h * h' = e \quad \Rightarrow \quad h \,.\, h' = 1 \quad \Rightarrow \quad h' = \frac{1}{h}$

$h' > 0 \quad \Rightarrow \quad h' \in H.$

Portanto, H é um subgrupo de $G = Q^*$.

UNIDADE III - HOMOMORFISMO DE GRUPOS

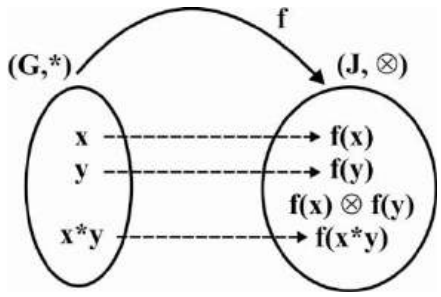
3.1. HOMOMORFISMO E CLASSIFICAÇÃO DO HOMOMORFISMO.

Definição:

Sejam os grupos **(G, ∗)** e **(J, ⊗)**.

Uma aplicação **f: G → J** é um ***homomorfismo*** de **G** em **J**, quando ela é compatível com as estruturas dos grupos, isto é, **f(*x* ∗ *y*) = f(*x*) ⊗ f(*y*)**, quaisquer que sejam ***x*** e ***y*** de **G**.

Simbolicamente:



Note que o primeiro membro desta relação, isto é, no termo **f(*x* ∗ *y*)** o composto ***x* ∗ *y*** é computado em **G** ao passo que no segundo membro desta relação, isto é, no termo **f(x) ⊗ f(y)**, o composto é de elementos de **J**. Com isto, entende–se uma aplicação de um sistema algébrico (grupo), em outro sistema algébrico semelhante (grupo), que conserva a estrutura.

Exemplos :

01. Sejam os grupos $(\Re, +)$ e $(\Re_+^*, .)$. A aplicação $f : \Re \to \Re_+^*$, definida por $f(x) = 2^x$ é um homomorfismo. De fato :
$f(a * b) = 2^{a+b} = 2^a . 2^b = f(a) \otimes f(b)$

02. Sejam os grupos $(\Re_+^*, .)$ e $(\Re, +)$. A aplicação $f : \Re_+^* \to \Re$, definida por $f(x) = \log(x)$ é um homomorfismo. De fato :
$f(m * n) = \log(m . n) = \log(m) + \log(n) = f(m) \otimes f(n)$

03. Sejam os grupos $(C^*, .)$ e $(\Re_+^*, .)$. A aplicação $f : C^* \to \Re_+^*$, definida por $f(z) = |z|$ é um homomorfismo. De fato :
$f(z_1 * z_2) = |z_1 . z_2| = |z_1| . |z_2| = f(z_1) \otimes f(z_2)$

04. A aplicação f: (ZxZ, +) → (ZxZ, +), definida por f(x,y) = (x – y, 0) é um homomorfismo. De fato :

f[(a,b) ∗ (c,d)] = f[(a,b) + (c,d)] = f[(a + c, b + d)] = **(**(a + c) – (b + d), 0**)**

f[(a,b) ∗ (c,d)] = **(**(a – b) + (c – d), 0 + 0**)** = (a – b, 0) + (c – d, 0) = f(a,b) ⊗ f(c,d)

05. Sejam os grupos multiplicativos G = $M_2(\Re)$ tal que det(A) ≠ 0; ∀A ∈ $M_2(\Re)$ e J = $\Re^*$. A aplicação f : $M_2(\Re) \to \Re_+^*$, definida por f(X) = det(X) é um homomorfismo. De fato :

f(A ∗ B) = det(A.B) = det(A) . det(B) = f(A) ⊗ f(B)

3.2. PROPRIEDADES DOS HOMOMORFISMOS

Seja **f: (G, ∗) → (J, ⊗)** um homomorfismo de grupos.

Teorema

A imagem **f(e_G)** do elemento neutro e_G do grupo **G** é o elemento neutro e_J do grupo **J**, isto é, **f(e_G) = e_J**.

Demonstração :

Para todo x elemento de G, temos :

$x * e_G = x$

$f(x * e_G) = f(x)$

$f(x) \otimes f(e_G) = f(x)$

$f(x) \otimes f(e_G) = f(x) \otimes e_J$

$f(e_G) = e_J$

c.q.d.

Teorema

A imagem do simétrico de qualquer elemento x do grupo **G** é igual ao simétrico da imagem de x, isto é, **f(x') = [f(x)]'** , ∀ x ∈ **G** .

Demonstração :

Para todo x elemento de G, temos :

$f(e_G) = e_J$

$f(x * x') = e_J$

$f(x) \otimes f(x') = e_J$

$f(x) \otimes f(x') = f(x) \otimes [f(x)]'$

$f(x') = [f(x)]'$

c.q.d.

Teorema

O homomorfismo transforma subgrupos de **G** em subgrupos de **J** .

Demonstração:

Seja (H, $*$) um subgrupo de (G, $*$) .

Afirmamos que (f(H), $\otimes$) é um subgrupo de (J, $\otimes$). De fato :

a) É óbvio que f(H) $\neq \varnothing$, pois $e_G \in H \Rightarrow f(e_G) = e_J \Rightarrow e_J \in f(H)$;

b) $\forall y_1, y_2 \in f(H)$, por definição, existem $x_1, x_2 \in H$ tais que $f(x_1) = y_1$ e $f(x_2) = y_2$. Assim, $y_1 \otimes y_2 = f(x_1) \otimes f(x_2) = f(x_1) \otimes f(x_2) = f(x_1 * x_2)$

Como $x_1 * x_2 \in H$, tem–se $y_1 \otimes y_2 \in f(H)$.

d) $\forall y \in f(H)$, por definição, existe $x \in H$ tais que $f(x) =$. Assim, $y' = f(x)' = f(x')$

Como $x' \in H$, tem–se $y' \in f(H)$.

Portanto, (f(H), $\otimes$) é um subgrupo de (J, $\otimes$) .

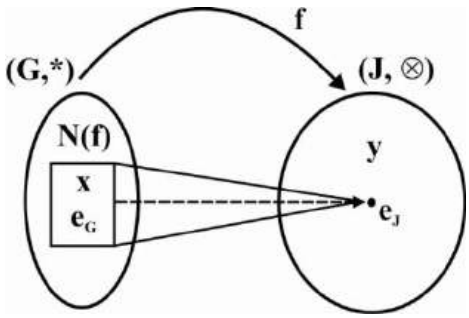
3.3. NÚCLEO DE UM HOMOMORFISMO

Definição:

Seja **f: (G, $*$) $\rightarrow$ (J, $\otimes$)** um homomorfismo de grupos e e_J o elemento neutro do grupo **J**. Chama–se ***núcleo*** ou ***Kernel*** do homomorfismo **f** ao conjunto **{ $x \in G$ | f(x) = e_J }**, indicado pela notação **N(f)** ou **Ker(f)** (leia–se núcleo ou Kernel de f), isto é :

$$N(f) = Ker(f) = \{ x \in G \mid f(x) = e_J \}$$

Em símbolos :



Exemplos :

01. Sejam os grupos ($\Re$, +) e ($\Re_+^*$, .) e o homomorfismo f : $\Re \rightarrow \Re_+^*$, definido por $f(x) = 2^x$.
Aplicando a condição para que um elemento x de G pertença ao núcleo de f, temos: $f(x) = e_J \Rightarrow 2^x = 1 \Rightarrow x = 0$
Assim, N(f) = {0}

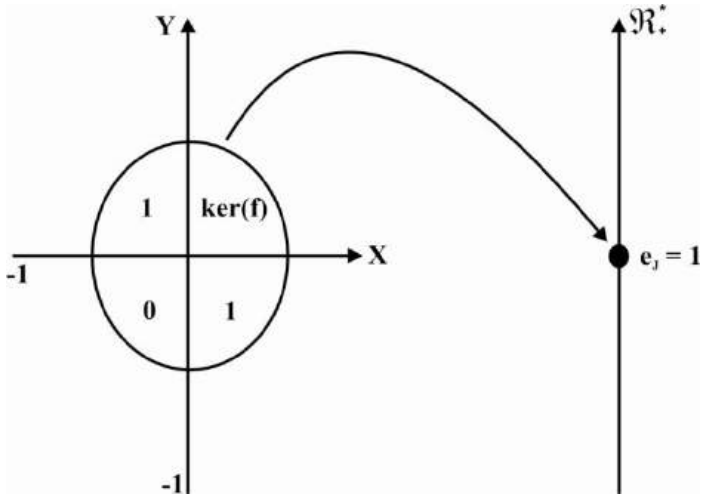
02. Sejam os grupos ($\Re_+^*$, .) e ($\Re$, +) e o homomorfismo f : $\Re_+^* \rightarrow \Re$, definido por $f(x) = \log(x)$. Então, $f(x) = e_J \Rightarrow \log(x) = 0 \Rightarrow x = 1$

Assim, N(f) = {1}

03. Sejam os grupos $(C^*, .)$ e $(\Re_+^*, .)$ e o homomorfismo $f : C^* \to \Re_+^*$, definido por $f(z) = |z|$, sendo $z = x + y.i$. Então $f(z) = e_J \Rightarrow |z| = 1 \Rightarrow x^2 + y^2 = 1$

Assim, $Ker(f) = \{z = x + y.i \in C \mid x^2 + y^2 = 1\}$

Geometricamente :



04. Consideremos o homomorfismo de grupos f: (ZxZ, +) → (ZxZ, +), definido por $f(x,y) = (x - y, 0)$. O Kernel de f é :

$f(x,y) = e_J \Rightarrow (x - y, 0) = (0,0) \Rightarrow x = y$

Assim, $Ker(f) = \{(x,y) \in ZxZ \mid x = y\}$

Sugerimos que o leitor faça uma interpretação geométrica do caso acima.

05. Seja o homomorfismo de grupos $f : (M_2(\Re), .) \to (\Re_+^*, .)$, definido por f(X) = det(X). Então, $f(X) = e_J \Rightarrow det(X) = 1$.

Assim, $Ker(f) = \{X \in M_2(\Re) \mid det(X) = 1\}$

Teorema

Seja **f: (G, ∗) → (J, ⊗)** um homomorfismo de grupos, então o núcleo de f é um subgrupo de G, isto é, o par **(N(f), ∗)** é um subgrupo do grupo **(G, ∗)** .

Demonstração :

a) Como $f(e_G) = e_J$, então $e_G \in N(f)$. Logo, $N(f) \neq \varnothing$.

b) Dados $x, y \in N(f)$, logo $f(x) = e_J$ e $f(y) = e_J$.

Assim, $f(x * y) = f(x) \otimes f(y)$

$f(x * y) = e_J \otimes e_J$

$f(x * y) = e_J$, o que implica em $x * y \in N(f)$.

c) Seja $x \in N(f)$, logo $f(x) = e_J$.

Assim, $f(x') = f(x)'$

$f(x') = e_J'$

$f(x') = e_J$, o que implica em $x' \in N(f)$.

Portanto, N(f) é um subgrupo de $(G, *)$.

- Sugerimos ao leitor que procure recordar quando uma aplicação é injetora, sobrejetora ou bijetora antes de dar continuidade neste texto.

3.4. HOMOMORFISMOS ESPECIAIS

Seja **f: (G, ∗) → (J, ⊗)** um homomorfismo de grupos.

MONOMORFISMO

Definição:

Diz–se que o homomorfismo **f** é um ***monomorfismo*** ou ***homomorfismo injetor*** quando a aplicação **f** é injetora .

EPIMORFISMO

Definição:

Diz–se que o homomorfismo **f** é um ***epimorfismo*** ou ***homomorfismo sobrejetor*** quando a aplicação **f** é sobrejetora .

ISOMORFISMO

Definição:

Isomorfismo ou ***homomorfismo bijetor*** é todo homomorfismo cuja aplicação **f** é bijetora .

ENDOMORFISMO

Definição :

Chama–se de ***endomorfismo*** a todo homomorfismo de (G, ∗) em si próprio .

AUTOMORFISMO

Definição:

Chama–se de ***automorfismo*** a todo endomorfismo cuja aplicação **f** seja bijetora .

Exemplos:

01. Sejam os grupos ($\Re$, +) e ($\Re_+^*$, .). A aplicação f : $\Re \to \Re_+^*$, definida por f(x) = 2^x é um isomorfismo.

02. Sejam os grupos ($\Re_+^*$, .) e ($\Re$, +). A aplicação f : $\Re_+^* \to \Re$, definida por f(x) = log(x) é um isomorfismo.

03. Sejam os grupos (C^*, .) e ($\Re_+^*$, .). A aplicação f : $C^* \to \Re_+^*$, definida por f(z) = $|z|$ é um epimorfismo.

04. A aplicação f: (ZxZ, +) $\to$ (ZxZ, +), definida por f(x,y) = ($x - y$, 0) é um endomorfismo.

05. Sejam os grupos ($\Re$, +) e ($\Re$, +). A aplicação f : $\Re \to \Re$, definida por f(x) = 2.x é um automorfismo.

06. A aplicação f: (Z, +) $\to$ (Q, +), definida por f(x,y) = 2.x é um monomorfismo.

Deixamos ao encargo do leitor mostrar que as aplicações são injetora, sobrejetora ou bijetora, conforme o caso.

UNIDADE IV - CLASSES LATERAIS

Sejam o grupo **(G, ∗)**, **H** um subgrupo de **G**¸ e **a** um elemento arbitrário de **G**.

4.1. CLASSE LATERAL À DIREITA

Definição:

A ***classe lateral à direita*** de **H** em **G** gerada por ***a***, denota–se por **H ∗ a**, é o seguinte subconjunto de **G** :

$$H * a = \{ h * a \mid h \in H \}$$

4.2. CLASSE LATERAL À ESQUERDA

Definição :

A ***classe lateral à esquerda*** de **H** em **G** gerada por ***a***, denota–se por **a ∗ H**, é o seguinte subconjunto de **G** :

$$\mathbf{a * H = \{ h * a \mid h \in H \}}$$

Exemplos:

01. Sejam o grupo multiplicativo **G = { – *i*, – 1, *i*, 1}** e o subgrupo **H = { – 1, 1}**.

Todas as possíveis operações do grupo figuram na tábua abaixo:

∗	– i	– 1	i	1
– i	– 1	i	1	– i
– 1	i	1	– i	– 1
i	1	– i	– 1	i
1	– i	– 1	i	1

A seguir apresentamos todas as classes laterais à esquerda e a direita de H em G.

$i * H = \{ x \in G \mid x = i * h ; h \in H \} = \{ -i, i \}$

$-i * H = \{ x \in G \mid x = -i * h ; h \in H \} = \{ -i, i \}$

$1 * H = \{ x \in G \mid x = 1 * h ; h \in H \} = \{ -1, 1 \}$

$-1 * H = \{ x \in G \mid x = -1 * h ; h \in H \} = \{ -1, 1 \}$

$H * i = \{ x \in G \mid x = h * i ; h \in H \} = \{ -i, i \}$

$H * -i = \{ x \in G \mid x = h * -i ; h \in H \} = \{ -i, i \}$

$H * 1 = \{ x \in G \mid x = h * 1 ; h \in H \} = \{ -1, 1 \}$

$H * -1 = \{ x \in G \mid x = h * -1 ; h \in H \} = \{ -1, 1 \}$

Observe que :

- As classes laterais são coincidentes ou disjuntas
- Se o elemento gerador da classe pertence ao subgrupo, então está classe é igual ao próprio subgrupo.

02. O grupo de Klein de ordem 4, K = { a, b, c, e} está representado na tábua abaixo :

∗	e	a	b	c
e	e	a	b	c

a	a	**e**	c	b
b	b	c	**e**	a
c	c	B	a	**e**

As classes laterais de H = { a, e } em G, são :

a ∗ H = { x ∈ G | x = a ∗ h ; h ∈ H } = { a, b, c, e }

b ∗ H = { x ∈ G | x = b ∗ h ; h ∈ H } = { a, b, c, e }

c ∗ H = { x ∈ G | x = c ∗ h ; h ∈ H } = { a, b, c, e }

e ∗ H = { x ∈ G | x = e ∗ h ; h ∈ H } = { a, b, c, e }

H ∗ a = { x ∈ G | x = h ∗ a ; h ∈ H } = { a, b, c, e }

H ∗ b = { x ∈ G | x = h ∗ b ; h ∈ H } = { a, b, c, e }

H ∗ c = { x ∈ G | x = h ∗ c ; h ∈ H } = { a, b, c, e }

H ∗ e = { x ∈ G | x = h ∗ e ; h ∈ H } = { a, b, c, e }

4.3. PROPRIEDADES DAS CLASSES LATERAIS

Teorema

Sejam **(H, ∗)** um subgrupo do grupo abeliano **(G, ∗)**, então as classes laterais à esquerda e à direita de **H** em **G**, gerada pelo elemento **a** de **G** coincidem.

Demonstração:

Considere as classes laterais a ∗ H = {a ∗ h | h ∈ H} e H ∗ a = {h ∗ a | h ∈ H }.

Assim, H ∗ a = { h ∗ a | h ∈ H } = { a ∗ h | h ∈ H } = a ∗ H, pois G é um grupo abeliano.

Teorema

Sejam **(H, ∗)** um subgrupo do grupo **(G, ∗)**, então todo elemento **a** de **G** pertence à sua classe lateral.

Demonstração:

Consideremos a classe lateral à direita H ∗ a de H em G, determinada por a ∈ G .

Sabemos que o elemento neutro *e* do grupo G pertence ao subgrupo H.

Logo, $a \in G$ e $e * a = a$ o que implica em $a \in H * a$.

De modo análogo, prova–se que $a \in a * H$.

Teorema

Sejam **(H, ∗)** um subgrupo do grupo **(G, ∗)**, e **a**, **b** elementos quaisquer de **G**, então as classes laterais à direita **H ∗ a** e **H ∗ b** (ou as classes laterais à esquerda **a ∗ H** e **a ∗ H**) de **H** em **G**, geradas por **a** e **b**, respectivamente, coincidem se, e somente se **a ∗ b' ∈ H** (ou **a' ∗ b ∈ H**).

Demonstração:

Consideremos que as classes laterais à direita sejam coincidentes, isto é, $H * a$ e $H * b$. Deste modo, existem $h_1, h_2 \in H$ tais que $h_1 * a = h_2 * b$, o que implica em $a * b' = h'_1 * h_2$. Como $h'_1 * h_2 \in H$, tem–se $a * b' \in H$.

Por outra parte, suponha que $a * b' \in H$. Assim, a classe lateral à direita determinada por $a * b'$ de H em G coincide com o subgrupo H. Deste modo, existem $h_3, h_4 \in H$ tais que $h_3 * (a * b') = h_4$, ou ainda $h_3 * a = h_4 * b$. Logo, todo elemento $h_3 * a \in H * a$ é igual a um elemento $h_4 * b \in H * b$, e vice-versa.

Portanto, $H * a = H * b$.

Por analogia, prova–se que $a * H = b * H$, se e somente se $a' * b \in H$.

Teorema

Sejam **(H, ∗)** um subgrupo do grupo **(G, ∗)**, e **a**, **b** elementos quaisquer de **G**, então as classes laterais à direita (ou as classes laterais à esquerda) de **H** em **G**, determinadas por **a** e **b** são disjuntas ou coincidentes.

Demonstração:

Consideremos as classes laterais à direita $H * a$ e $H * b$ de H em G, determinadas por a e b, respectivamente.

Suponha que exista um elemento x de G tal que $x \in H * a$ e $x \in H * b$.

Logo existem $h_1, h_2 \in H$ tais que :

$h_1 * a = x = h_2 * b$ ou ainda

$h_1 * a = h_2 * b$

$h'_1 * (h_1 * a) * b' = h'_1 * (h_2 * b) * b'$

$a * b' = h'_1 * h_2$

O fato de que $h'_1 * h_2 \in H$ implica em $a * b' \in H$. Portanto, $H * a = H * b$

De modo análogo, demonstra-se que vale para as classes laterais à esquerda.

Lema

Sejam **(G, *)** um grupo e **H** um subgrupo de **G** e **a**, **b ∈ G**, com **a ≠ b**. Então existe uma correspondência biunívoca entre **H * a** e **H * b** (ou **a * H** e **b * H**) .

Demonstração:

Definamos a seguinte aplicação :

$f : H * a \rightarrow H * b$

$h * a \rightarrow h * b$

$f(h * a) = h * b$

Afirmamos que $f : H * a \rightarrow H * b$ é bijetora. De fato :

a) Seja $f(h_1 * a) = f(h_2 * a) \Rightarrow h_1 * b = h_2 * b \Rightarrow h_1 = h_2$
logo, $h_1 * a = h_2 * a$. $\therefore$ f é injetora.

b) Dado $h * b \in H * b$. Então existe $h * a \in H * a$ tal que $f(h * a) = h * b$, pela definição de f. $\therefore$ f é sobrejetora.

Teorema de Lagrange

A ordem de qualquer subgrupo (H, *) de um grupo finito (G, *) divide a ordem do grupo (G, *).

Demonstração:

Pelo teorema sobre partições em um conjunto, tem–se que as classes laterais à direita (ou à esquerda) de H em G, decompõem G em classes laterais mutuamente disjuntas. Por outro lado, sabemos que entre duas classes laterais existe sempre uma correspondência bijetora, isto é, $H * a \leftrightarrow H * b$, $\forall a, b \in G$, e mais ainda $H * a \leftrightarrow H * b \leftrightarrow H * e = H$. Logo, como G é finito, o número de classes laterais multiplicado pela quantidade de elementos em

H, fornece o número de elementos de G, isto é, k.o(H) = o(G), onde k corresponde ao número de classes laterais mutuamente disjuntas, ou em símbolos :

$G = (a_1 * H) \cup (a_2 * H) \cup ... \cup (a_k * H) \Rightarrow o(G) = o(H) + o(H) + ... + o(H) \Rightarrow o(G) = k \, . \, o(H) \Leftrightarrow o(H) \mid o(G)$

- A recíproca do Teorema de Lagrange é falsa, pois um grupo finito não tem necessariamente um subgrupo cuja ordem seja um divisor da ordem do grupo.
- Se a ordem do grupo for um número primo, então os subgrupos são triviais.
- O teorema de Lagrange é de fundamental importância porque introduz relações aritméticas na teoria dos grupos.

4.4. SUBGRUPO NORMAL

Definição:

Seja **(H, ∗)** um subgrupo do grupo **(G, ∗)**. Diz–se que **H** é um ***subgrupo normal*** ou um ***subgrupo invariante*** de **G** quando a condição **$a * H = H * a$** , **$\forall \, a \in G$** é verificada, denota–se por **$H \triangleleft G$**.

Se (G, ∗) é um grupo abeliano, então todo subgrupo de G é um subgrupo normal, mas a recíproca é falsa.

Deixamos ao encargo do leitor apresentar exemplos de subgrupos normais.

UNIDADE V - ANÉIS E CORPOS

5.1. ANEL

Definição:

Seja **A** um conjunto não vazio (**$A \neq \varnothing$**) munido de duas operações internas ⊕ e ⊗.

Diz–se que a terna **(A, ⊕, ⊗)** é um ***anel*** quando as operações internas ⊕ e ⊗ possuem as seguintes propriedades :

(A_1) O par **(A, ⊕)** é um grupo abeliano;

(A_2) ∀a, b, c ∈ A, tem–se **$a \otimes (b \otimes c) = (a \otimes b) \otimes c$**

(A_3) ∀a, b, c ∈ A, tem–se : **$a \otimes (b \oplus c) = a \otimes b \oplus a \otimes c$**

$(b \oplus c) \otimes a = b \otimes a \oplus c \otimes a$

Exemplos:

01. As ternas (Z, +, .); (Q, +, .); ($\Re$, +, .) e (C, +, .) são anéis, pois, para cada uma delas, são válidas as três seguintes condições:

    (A1) Os pares (Z, +); (Q, +); ($\Re$, +) e (C, +) são grupos abelianos;

    (A2) Os pares (Z, .); (Q, .); ($\Re$, .) e (C, .) são semi–grupos;

    (A3) A multiplicação (.) em Z, Q, $\Re$ e C é distributiva em relação a adição (+).

02. A terna ($2.Z$, +, .), onde $2.Z$ denota o conjunto dos números inteiros pares, é um anel, pois, são válidas as três seguintes condições:

    (A1) O par ($2.Z$, +) é um grupo abeliano;

    (A2) O par ($2.Z$, .) é um semi–grupo;

    (A3) A multiplicação (.) em $2.Z$ é distributiva em relação a adição (+).

03. Seja $M_2(\Re)$ o conjunto de todas as matrizes quadradas de ordem 2. A terna ($M_2(\Re)$, +, .) é um anel, pois, temos :

    (A1) O par ($M_2(\Re)$, +) é um grupo abeliano;

    (A2) O par ($M_2(\Re)$, .) é um semi–grupo;

    (A3) A multiplicação (.) em $M_2(\Re)$ é distributiva em relação a adição (+) .

04. A terna ({0}, +, .) é um anel, porque ({0}, +) é um grupo abeliano; ({0}, .) é um semi–grupo e a multiplicação (.) é distributiva em relação à adição (+).

05. Seja $A = \Re^{\Re} = \{ f \mid f : \Re \to \Re \}$. Dadas duas funções quaisquer $f, g \in A$, definindo $f + g$ e $f.g$ da seguinte forma :

$$(f + g) : \Re \to \Re \qquad (f + g)(x) = f(x) + g(x)$$

$$(f.g) : \Re \to \Re \qquad (f.g)(x) = f(x).g(x)$$

    Nessas condições A é um anel.

5.2. ANÉIS COMUTATIVOS, ANÉIS COM UNIDADE E ANÉIS DE INTEGRIDADE.

ANE L COMUTATIVO

Definição:

Diz–se que o anel **(A, ⊕, ⊗)** é um ***anel comutativo***, quando a operação ⊗ é comutativa, isto é, ∀a, b ∈ A, tem–se a ⊗ b = b ⊗ a.

ANEL COM UNIDADE

Definição:

Diz–se que o anel **(A, ⊕, ⊗)** é um ***anel com unidade***, quando a operação ⊗ admite elemento neutro em **A**, isto é, **∀a ∈ A**, tem–se $\mathbf{a \otimes 1_A = 1_A \otimes a = a}$.

- O elemento neutro em relação a operação ⊕ será denotado por $\mathbf{0_A}$, enquanto que, o elemento neutro em relação a operação ⊗ será denotado por $\mathbf{1_A}$.

ANEL COMUTATIVO COM UNIDADE

Definição:

Diz–se que o anel **(A, ⊕, ⊗)** é um ***anel comutativo com unidade***, quando a operação ⊗ for comutativa e admitir elemento neutro em **A**.

ANEL DE INTEGRIDADE

Definição:

Diz–se que o anel comutativo com unidade **(A, ⊕, ⊗)** é um ***anel de integridade***, quando ∀a, b ∈ A, tem–se $a \otimes b = 0_A \Rightarrow a = 0_A$ ou $b = 0_A$, isto é, vale a lei do anulamento do produto.

Se **a** e **b** são elementos não nulos do anel **A** tais que $\mathbf{a \otimes b = 0_A}$ ou $\mathbf{b \otimes a = 0_A}$, dizemos que **a** e **b** são ***divisores próprios do zero*** em **A**.

Exemplos :

01. Os anéis (Z, +, .); (Q, +, .); ($\Re$, +, .) e (C, +, .) são exemplos clássicos de anéis de integridade.

02. O anel ($M_2(\Re)$, +, .) não é de integridade, pois, além de não ser comutativo apresenta divisores próprios do zero, conforme abaixo :

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

embora, $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} . \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$

5.4. SUBANÉIS

Definição:

Sejam **(A, ⊕, ⊗)** é um anel e **L** um subconjunto não vazio de **A**. Diz-se que **L** é um **subanel** quando:

a) **L** é fechado para as operações que dotam o conjunto **A** da estrutura de anel;

b) **(L, ⊕, ⊗)** também é um anel.

Exemplo:

Considerando-se as operações usuais sobre os conjuntos numéricos temos que:

a) Z é subanel de Q, R e C;

b) Q é subanel de R e C;

c) R é subanel de C.

Proposição:

Sejam **(A, ⊕, ⊗)** é um anel e **L** um subconjunto não vazio de **A**. Então L é um subanel de A se, e somente se, $a \oplus b$' e $a \otimes b \in \mathbf{L}$, sempre que $a,b \in \mathbf{L}$.

5.5. CORPO

Definição:

Chama–se ***corpo*** todo anel comutativo **(C, ⊕, ⊗)** com elemento unidade e tal que todo elemento não nulo de C é inversível para a operação ⊗ .

Em outras palavras, ***corpo*** é toda terna ordenada **(C, ⊕, ⊗)** que satisfaz as seguintes condições :

(C_1) **(C, ⊕)** é um grupo abeliano;

(C_2) **(C^*, ⊗)** é um grupo abeliano;

(C_3) A operação ⊗ é distributiva em relação à operação ⊕ .

Exemplos :

01. Os anéis (*Q*, +, .); (ℜ, +, .) e (*C*, +, .) são corpos, denominados, respectivamente, corpo dos números racionais, corpo dos números reais e corpo dos números complexos, pois, são válidas as condições:
(A1) Os pares (*Q*, +); (ℜ, +) e (*C*, +) são grupos abelianos;
(A2) Os pares (*Q*, .); (ℜ, .) e (*C*, .) são grupos abelianos;
(A3) A multiplicação (.) em *Q*, ℜ e *C* é distributiva em relação a adição (+).

02. A terna (*Z*, +, .) é um anel mas não é um corpo. Deixamos ao encargo do leitor verificar porque (*Z*, +, .) não é um corpo.

03. A terna (C = { a + b $\sqrt{3}$ | a, b ∈ *Q* }, +, .) é um corpo, pois, as três condições para que um conjunto não vazio seja um corpo são satisfeitas.

04. A terna (C = { a, b, c }, ⊕, ⊗), com as operações ⊕ e ⊗ definidas pelas tábuas abaixo é um corpo.

⊕	**a**	**b**	**c**
a	a	b	c
b	b	c	a
c	c	a	b

⊗	**a**	**b**	**c**
a	a	a	a
b	a	b	c
c	a	c	b

05. A terna ($\Re x\Re$, $\oplus$, $\otimes$), com as operações $\oplus$ e $\otimes$ abaixo definidas é um corpo.

(a,b) $\oplus$ (c,d) = (a + c, b + d) e (a,b) $\otimes$ (c,d) = (ad – bc ,ad + bc)

Note que os pares ($\Re^2$, $\oplus$) e ($\Re^2$, $\otimes$) são grupos abelianos e que, a operação $\otimes$ e distributiva em relação à operação $\oplus$.

Teorema

Todo corpo **(C, $\oplus$, $\otimes$)** não possui divisores de zero.

Demonstração:

Devemos provar que da igualdade a.b = 0 implica em a = 0 ou b = 0, quaisquer que sejam os elementos a, b $\in$ C.

Se a = 0, não há o que demonstrar.

Se a $\neq$ 0, então pela definição de corpo, o elemento a $\in$ C é inversível, isto é, possui inverso $a^{-1} \in C$.

Assim, a.b = 0 $\Rightarrow$ $a^{-1}.a.b = a^{-1}.0$ $\Rightarrow$ $1_A.b = 0$ $\Rightarrow$ b = 0 .

Teorema

Todo corpo **(C, $\oplus$, $\otimes$)** é um anel de integridade.

Demonstração:

De fato, de acordo com a definição de corpo e teorema acima, (C, $\oplus$, $\otimes$) é um anel comutativo com elemento unidade e sem divisores de zero, portanto, (C, $\oplus$, $\otimes$) é um anel de integridade.

EXERCÍCIOS

01. Dados os conjuntos A = {a, b} ; B = {2, 3} e C = {3, 4} . Calcule:
    a) A x (B ∪ C)
    b) (A x B) ∪ (A x C)
    c) A x (B ∩ C)
    d) (A x B) ∩ (A x C)
    e) A x (B – C)
    f) A x (C – B)

02. Represente A x B e B x A nos seguintes casos :
    a) A = $\{x \in \Re \mid 2 < x < 5\}$ e B = $\{ y \in \Re \mid 1 \leq y \leq 6 \}$.
    b) A = $\{x \in \Re \mid 1 \leq x < 5\}$ e B = $\{ y \in \Re \mid 1 < y \leq 5 \}$.
    c) A = $\{x \in \Re \mid -2 \leq x < 5\}$ e B = $\{ y \in \Re \mid 1 \leq y < 6 \}$.
    d) A = $\{x \in \Re \mid -3 < x < 3\}$ e B = $\{ y \in \Re \mid -1 < y < 1 \}$.

03. Sejam os conjuntos A = { 0, 2, 4, 6, 8} e B = { 1, 3, 5, 9}. Enumerar os elementos das relações abaixo definidas, determinando seu domínio, a imagem e a relação inversa:
    a) $R_1 = \{(x,y) \in AxB \mid y = x + 1\}$
    b) $R_2 = \{(x,y) \in AxB \mid x \leq y\}$
    c) $R_3 = \{(x,y) \in AxB \mid y = x^2 + 1\}$
    d) $R_4 = \{(x,y) \in AxB \mid y \mid (x + 1)\}$ " $y \mid (x + 1) \Rightarrow y$ divide $(x + 1)$"

04. Sabendo-se que A é um conjunto com 5 elementos e R = {(0,1); (1,2); (2,3); (3,4)} é ma relação sobre A. Pede-se obter :
    a) Os elementos de A
    b) O domínio e a imagem de R
    c) Os elementos, domínio e imagem de R^{-1}

05. Sejam A = $\boldsymbol{N}$ e a relação R = $\{(x,y) \in AxA \mid 2x + y = 10\}$. Determine o domínio e a imagem de R e R^{-1}.

06. Seja A = {1, 2, 3}. Classifique as relações abaixo em reflexiva, simétrica, transitiva e anti-simétrica :
    a) $R_1 = \{(1,2); (1,1); (2,2); (2,1); (3,3)\}$
    b) $R_2 = \{(1,1); (2,2); (3,3); (1,2); (2,3)\}$
    c) $R_3 = \{(1,1); (2,2); (1,2); (2,3); (3,1)\}$
    d) $R_4 = A^2$
    e) $R_5 = \varnothing$

07. Dê um exemplo de uma relação sobre o conjunto A { a, b, c, d, e} que :
    a) Seja apenas reflexiva
    b) Seja apenas simétrica
    c) Seja apenas simétrica e anti-simétrica
    d) Não seja nem simétrica e nem anti-simétrica

08. Sejam R e S relações sobre o mesmo conjunto A. Prove que:
    a) Se R e S são simétricas, então R ∩ S e R ∪ S são simétricas.
    b) Se R e S são transitivas, então R ∩ S é transitiva.
    c) $R^{-1} \cap S^{-1} = (R \cap S)^{-1}$
    d) $R^{-1} \cup S^{-1} = (R \cup S)^{-1}$
    e) Se R é transitiva, então R^{-1} também é transitiva.
    f) Qualquer que seja R, tem-se $R \cup R^{-1}$ é simétrica

09. Quais das relações abaixo são de equivalência sobre o conjuntos dos inteiros positivos?
    a) $xRy \Leftrightarrow x + y = 12$
    b) $xRy \Leftrightarrow mdc(x, y)$
    c) $xRy \Leftrightarrow x \mid y$
    d) $xRy \Leftrightarrow \exists$ inteiro k tal que $x - y = 4k$

10. Sejam A = $\{x \in Z \mid \mid x \mid \leq 4\}$ e a relação R definida por $xRy \Leftrightarrow x + \mid x \mid = y + \mid y \mid$. Determinar o conjunto quociente A/R.

11. Sejam A = $\{x \in Z \mid \mid x \mid \leq 5\}$ e a relação R definida por $xRy \Leftrightarrow x^2 + 2x = y^2 + 2y$. Determinar o conjunto quociente A/R.

12. Sejam M um conjunto não vazio, A = $\wp$(M) (conjunto das partes de M) e as relações R definida por XRY ⇔ X ∩F = Y∩F e XSY ⇔ X∪F = Y∪F, onde F é um subconjunto fixo de M. Verifique se as relações R e S são de equivalência.

13. Mostre que a relação R de finida por $xRy \Leftrightarrow x - y \in Q$ (conjunto dos números racionais) é

uma relação de equivalência sobre A = $\Re$ e descreva as classes geradas por $\frac{1}{2}$ e $\sqrt{2}$.

14. Mostre que a relação R de finida por (a + b.*i*)R(c + d.*i*) $\Leftrightarrow$ $a^2 + b^2 = c^2 + d^2$ é uma relação de equivalência sobre A = *C* (conjunto dos números complexos) e descreva as classes geradas por $1 + i$ e $1 - i$.

15. Seja A o conjunto das retas de um plano π. Quais das relações abaixo definidas são relações de equivalência ou de ordem em A ?
    a) xR$y \Leftrightarrow x // y$
    b) xR$y \Leftrightarrow x \perp y$

16. Verifique se a relação (a,b) R (c,d) $\Leftrightarrow$ a.d = b.c em A = ZxZ é uma relação de equivalência.

17. Dado o conjunto A = *C* e seja os números complexos x = a + b.*i* e y = c + d.*i* de *C*. Verifique se a relação xR$y \Leftrightarrow a \le c$ e $b \le d$ é uma relação de ordem parcial em *C*.

18. Sejam os conjuntos $B \neq \varnothing$ e A = $\wp$(B) e a relação XRY $\Leftrightarrow$ X $\subset$ Y em A. Verifique se a relação R é uma relação de ordem em A.

19. Faça o diagrama simplificado das seguintes relações de ordem no conjunto A = {1, 2, 4, 5, 10, 20}. Sendo: a) Ordem habitual. b) Ordem por divisibilidade.

20. Faça o diagrama simplificado da relação de ordem por inclusão em A = $\wp$({a,b}).

21. Faça o diagrama simplificado da relação de ordem por divisibilidade no conjunto A = {2,3,5,10,15,30} e determine os limites superiores, os limites inferiores, o supremo, o ínfimo, o máximo, o mínimo, o maximal e o minimal, considerando B = {6, 10}.

22. Faça o diagrama simplificado da relação de ordem por divisibilidade no conjunto A = {1,2,3,4,6,9,12,18,36} e determine os limites superiores, os limites inferiores, o supremo, o ínfimo, o máximo, o mínimo, o maximal e o minimal, considerando B = {2,4,6}.

23. Seja B = $\{x \in Q \mid 0 \le x^2 \le 2\}$ um subconjunto de A = Q, em que se considera a relação de ordem habitual. Determine os limites superiores, os limites inferiores, o supremo, o ínfimo, o máximo, o mínimo, o maximal e o minimal.

24. Faça o diagrama simplificado da relação de ordem por inclusão em A = $\wp$({a,b,c}) e determine os limites superiores, os limites inferiores, o supremo, o ínfimo, o máximo, o mínimo, o maximal e o minimal, considerando B = {{a}, {a,b}, {a,c}}.

25. A aplicação f: Qx$Q \to Q$, definida por f(x,y) = $\frac{x}{y}$ é uma lei de composição interna ?

26. Seja $M_2(\Re)$ o conjunto das matrizes quadradas de elementos reais. A operação definida em $M_2(\Re)$ por X $*$ Y = X . Y é uma lei de composição interna ?

27. Seja a operação interna $x*y = x + y$ em A = *N*. Os elementos de *N* são todos regulares ?

28. Construa a tábua da operação $x*y$ = mdc(x,y) em A = {1, 3, 5, 15}.

29. Construa a tábua da operação X$*$Y = X $\subset$ Y em A = { M, N, P, Q }, com M $\subset$ N $\subset$ P $\subset$ Q.

30. Em cada um dos casos abaixo, considere a operação $*$ definida sobre A e verifique em quais vale as propriedade associativa, comutativa, elemento neutro, elemento simetrizável e elemento regular :
    a) A = $\Re$ e $x * y = \frac{x + y}{2}$.
    b) A = $\Re$ e $x * y = \sqrt{x^2 + y^2}$.
    c) A = $\Re$ e $x * y = x \,.\, y + 2.x$
    d) A = ZxZ e (a,b)$*$(c,d) = (a + c, b.d)
    e) A = ZxZ e (a,b)$*$(c,d) = (a . c , 0)

31. Qual a condição que deve ser imposta aos inteiros p e q de modo que a operação $x * y$ = p.x + q.y , em A = *Z*, seja :
    a) Associativa
    b) Comutativa
    c) Admita elemento neutro

32. Verifique se o conjunto
    A = $\left\{ \begin{bmatrix} \cos(\theta) & \text{sen}(\theta) \\ -\text{sen}(\theta) & \cos(\theta) \end{bmatrix} \mid \theta \in \Re \right\}$ é um subconjunto fechado de $M_2(\Re)$ para a multiplicação usual de matrizes.

33. Construa a tábua da operação $*$ sobre o conjunto A = { 1, 2, 3, 4} de modo que :
    a) A operação seja comutativa
    b) O elemento neutro seja e = 1
    c) U_*(A) = A
    d) R_*(A) = A

e) $2 * 3 = 1$

34. Verifique se a operação $*$ definida pela tábua abaixo em A = { 1, 2, 3, 4} é um grupo abeliano:

*	1	2	3	4
1	3	4	1	2
2	4	3	2	1
3	1	2	3	4
4	2	1	4	3

35. Verifique se o conjunto G = { $a + b.\sqrt{2}$ | a, b $\in Q$ } com a operação $x * y = x . y$ é um grupo abeliano.
36. Seja $A = \Re^{\Re} = \{ f \mid f : \Re \to \Re \}$. Dadas duas funções quaisquer f, g $\in$ A, definindo f + g e f.g da seguinte forma :

    $(f + g) : \Re \to \Re \quad (f + g)(x) = f(x) + g(x)$
    $(f.g) : \Re \to \Re \quad (f.g)(x) = f(x).g(x)$

    Verifique se os pares (A, +) e (A, .) são grupos abelianos. Justifique a resposta, caso não seja grupo abeliano.

37. Construa a tábua do grupo G = {1, 2, 3, 4, 5, 6} de ordem 6, sabendo que :
    a) G é abeliano
    b) O neutro é $e = 5$
    c) $1 * 6 = 2 * 4 = 5$
    d) $1 * 4 = 2 * 3 = 6$
    e) $1 * 3 = 2 * 2 = 4$
    f) $3 * 4 = 1$

38. Prove que, se no grupo (G, $*$) existe x tal que $x * x = x$, então x é o elemento neutro.

39. Mostre que o conjunto

    $$G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}; \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}; \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}; \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$$

    com a operação de multiplicação usual de matrizes é um grupo abeliano.

40. O par (G = { 2^k | k $\in Z$ }, $*$) é um grupo abeliano, sendo $x * y = x . y$.

41. Prove que, se no grupo (G, $*$) todo elemento x e tal que $x * x = e$, então G é abeliano.

42. Abaixo está relacionado um grupo G, a operação $*$ e um subconjunto H. Quais destes subconjuntos são subgrupos :
    a) $G = M_2(\Re)$; $X * Y = X.Y$ e

    $$H = \left\{ \begin{bmatrix} \cos(\theta) & \text{sen}(\theta) \\ -\text{sen}(\theta) & \cos(\theta) \end{bmatrix} \mid \theta \in \Re \right\}$$

    .
    b) G = Q – {1}; $x * y = x + y – x.y$ e H = 2.Z = { 0, ±2, ±4, ±6, ±8, ±...}

    c) G = Z; $x * y = x + y$ e H = 2.Z = { 0, ±2, ±4, ±6, ±8, ±...}

    d) $G = C^*$; $z_1 * z_2 = z_1 . z_2$ e H = { z $\in C$ | |z| = 2 }

    e) $G = \Re$; $x * y = x + y$ e H = N .

43. Provar que, se H_1 e H_2 são subgrupos do grupo (G, $*$), então $H_1 \cap H_2$ é um subgrupo do grupo G.
44. Mostre que, se G é um grupo e $x * x = 1$, então G é abeliano.

45. Mostre que, se x é elemento grupo e $x * x = x$, então x é o elemento neutro.

46. Sejam a, b, c elementos de um grupo G. Prove que o simétrico de $a*b*c$ é $c'*b'*a'$. Obtenha x $\in$ G, tal que $a*b*c*x*b = a*b*x$.

47. Verifique se $H_1 = \{x \in Q \mid x > 0\}$ e $H_2 = \left\{ \frac{1+2m}{1+2n} : m, n \in Z \right\}$ são subgrupos do grupo multiplicativo Q^*.

48. Verifique se $H_1 = \{a + b\sqrt{2} \in \Re^* \mid a, b \in Q\}$ e $H_2 = \left\{ a + b\sqrt[3]{2} \in R^* : a, b \in Q \right\}$ são subgrupos do grupo multiplicativo $\Re^*$.

49. Provar que, se H_1 e H_2 são subgrupos de um grupo (G, $*$), então $H_1 \cup H_2$ é um subgrupo do grupo G se, e somente se, $H_1 \subset H_2$ ou $H_2 \subset H_1$.

50. Verifique se $H_1 = \{\cos(\theta) + i.\text{sen}(\theta) \mid \theta \in \Re\}$ e $H_2 = \{z \in C : |z| = 2\}$ são subgrupos do grupo multiplicativo C^*.

51. Seja G um grupo e a um elemento de G. Prove que N(a) = { { $x \in G \mid a*x = x*a$ } é um subgrupo de G.

52. O subconjunto H = { 6^n | n $\in Z$ } é um subgrupo do grupo (Q^*, .).

53. Verifique se as aplicações abaixo definidas são homomorfismos de grupos, em caso afirmativo classifique–a :
    a) $f : (\Re^*, .) \to (\Re^*, .)$, definida por $f(x) = |x|$
    b) $f : (\Re, +) \to (\Re, +)$, definida por $f(x) = x + 10$
    c) $f : (Z, +) \to (ZxZ, +)$, definida por $f(x) = (x , 0)$
    d) $f : (\Re, +) \to (\Re^*, .)$, definida por $f(x) = 10^x$
    e) $f : (\Re^*, .) \to (\Re, +)$, definida por $f(x) = \log(x)$
    f) $f : (C^*, .) \to (C^*, .)$, definida por $f(z) = \overline{z}$
    g) $f : (C^*, .) \to (C^*, .)$, definida por $f(z) = z^2$
    h) $f : (C^*, .) \to (C^*, .)$, definida por $f(z) = -\frac{1}{z}$
    i) $f : (C^*, .) \to (C^*, .)$, definida por $f(z) = - z$
    j) $f : (Z, +) \to (C^*, .)$, definida por $f(n) = i^n$
    k) $f : (\Re^*, .) \to (\Re^*, .)$, definida por $f(x) = x^3$

54. Verifique se $f : (Z, +) \to (2.Z, +)$, definida por $f(x) = 2.x$ é um isomorfismo.

55. Mostre que o par $(G = \{ a^n \mid n \in Z \}, .)$ é um grupo abeliano e que $f : (Z, +) \to (G, .)$ é um isomorfismo.

56. Dado o grupo $(G, *)$ e seja a um elemento fixo do grupo G. Prove que a aplicação f: G $\to$ G definida por $f(x) = a * x * a'$ é um isomorfismo.

57. Construa a tábua de um grupo G = {e, a, b, c} que seja isomorfo ao grupo multiplicativo J = { – 1, – i, 1, i}.

58. Prove que um grupo G é abeliano se, e somente se, f: G $\to$ G, definida por $f(x) = x'$ é um homomorfismo.

59. Determinar todas as classes laterais do subgrupo H = 2.Z no grupo aditivo G = Z.

60. Determinar todas as classes laterais do subgrupo H = 3.Z no grupo aditivo G = Z.

61. Todas as possíveis operações do grupo G = { 3, 5, 7, 9} estão representadas na tábua abaixo. Determine todas as classes laterais geradas pelo subgrupo H = {3, 7} em G.

*	**3**	**5**	**7**	**9**
3	3	5	7	9
5	5	7	9	3
7	7	9	3	5
9	9	3	5	7

62. Seja f: G $\to$J um homomorfismo sobrejetor de grupos. Se H é um subgrupo normal de G, mostre que f(H) é um subgrupo normal de J..

63. O conjunto G = $\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}; \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}; \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}; \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$ com as operações usuais de adição e multiplicação de matrizes é um anel de integridade

64. Verifique se a terna ordenada (Z, $\oplus$, $\otimes$) com as operações abaixo definidas é um anel comutativo com unidade:
    $a \oplus b = a + b - 1$ e $a \otimes b = a + b - a.b$

65. Verifique se a terna ordenada (ZxZ, $\oplus$, $\otimes$) com as operações abaixo definidas é um anel comutativo com unidade:
    $(a,b) \oplus (c,d) = (a + c , b + d)$ e
    $(a,b) \otimes (c,d) = (a.c , b.d)$

    Porque não é um anel de integridade? Existem divisores do zero?

66. Verifique se a terna ordenada ($\Re$, $\oplus$, $\otimes$) com as operações abaixo definidas é um corpo:
    $a \oplus b = a + b - 1$ e $a \otimes b = a + b - a$

67. Mostre que (Q, $\oplus$, $\otimes$) com as operações abaixo definidas é um anel comutativo com unidade:
    $x \oplus y = x + y - 3$ e
    $x \otimes y = x + y - \frac{x.y}{3}$

68. Seja E um conjunto não vazio. Mostre que ($\wp$(E), $\oplus$, $\otimes$) com as operações abaixo definidas é um anel comutativo com unidade:

    $X \oplus Y = (X \cup Y) - (X \cap Y)$ e
    $X \otimes Y = X \cap Y$

69. Verifique se $L = \{a + b\sqrt{2} \mid a, b \in Q\}$ é subanel de $A = \Re$.

70. Prove que $L = M_2(Z)$ é um subanel de $A = M_2(Q)$.

BIBLIOGRAFIA:

ALENCAR FILHO, Edgard de. **Teoria Elementar dos Conjuntos**. Nobel. São Paulo, 1990.

ALENCAR FILHO, Edgard de. **Elementos de Álgebra Abstrata**. Nobel. São Paulo, 1979.

AZEVEDO, Alberto & PICCININI, Renzo. **Introdução à teoria dos grupos**. IMPA, Rio de Janeiro, 1969.

DOMINGUES, Higino & IEZZI, Gelson. **Álgebra Moderna**. Atual. São Paulo, 1995.

GARCIA, Arnaldo & LEQUAIN, Yves. **Álgebra: um curso de introdução**. IMPA. Rio de Janeiro, 1988.

HERNSTEIN, I. N. **Topics in Algebra**. Tradução: Adalberto P. Bergamasco e L.H. Jacy Monteiro. Polígono. São Paulo, 1970.

SIMIS, Aron. **Introdução à Álgebra.** IMPA – Monografias de Matemática. Rio de Janeiro, 1976.


UEPA
UNIVERSIDADE DO ESTADO DO PARÁ