# Tópico 0 - Introdução a Estruturas Algébricas

João B. Florindo

Instituto de Matemática, Estatística e Computação Científica
Universidade Estadual de Campinas - Brasil
jbflorindo@ime.unicamp.br

# Outline

# Conceitos iniciais

Um **par ordenado** é uma lista com dois elementos genéricos $a, b \in X$, tal que um deles assume a posição de "primeiro" ($a$ no caso) e outro de "segundo" (no caso $b$) e de modo também que:

$$(a, b) = (c, d) \Leftrightarrow a = b \text{ e } c = d$$

EXEMPLO: Coordenadas cartesianas $(x, y)$.

Dados dois conjuntos $A$ e $B$, o conjunto de pares ordenados $(a, b)$ tais que $a \in A$ e $b \in B$ é chamado de **produto catesiano** de $A$ e $B$, $A \times B$. Note que em geral $A \times B \neq B \times A$.

Sejam $A$ e $B$ dois conjuntos com produto cartesiano $A \times B$. Um subconjunto de $A \times B$ é chamado de **relação binária** ou simplesmente **relação** entre $A$ e $B$.

# Conceitos iniciais

Uma **função** é um tipo especial de relação $F$ entre dois conjuntos $A$ e $B$, tal que só podemos ter $(a, b) \in F$ e $(a, b') \in F$ se $b = b'$. O conjunto $A$ é chamado de domínio de $F$ e $B$ de contradomínio de $F$

Escreve-se $F : A \rightarrow B$ e lê-se função $F$ de $A$ em $B$. Veremos também notação $F \in B^A$.

EXEMPLO: $f(x) = e^x$
CONTRA-EXEMPLO: Equação da circunferência $x^2 + y^2 = 1$ - Para um mesmo $x$ tenhos dois valores distintos de $y$.

# Outline

# Conceitos iniciais

Seja $X$ um conjunto não-vazio. Uma **relação de ordem parcial** ou **relação de ordem** em $X$ é uma relação $R \subset X \times X$ satisfazendo as seguintes condições:

1. Reflexividade: $(a, a) \in R, \forall a \in X$.
2. Transitividade: se $(a, b) \in R$ e $(b, c) \in R$, então $(a, c) \in R$.
3. Antissimetria: se $(a, b) \in R$ e $(b, a) \in R$, então obrigatoriamente $a = b$.

Se o conjunto $X$ possui uma relação de ordem parcial $R$, $X$ é dito ser um **conjunto parcialmente ordenado** por $R$ (*poset* em inglês).

O fato de que $(a, b) \in R$ é denotado $a \preceq_R b$ ou simplesmente $a \preceq b$.

# Conceitos iniciais

EXEMPLO 1: Seja $X$ um conjunto e $\mathbb{P}(X)$ a coleção de todos os seus subconjuntos. Então para quaisquer $A, B \subset X$ podemos estabelecer a relação de ordem $R$ tal que $A \preceq_R B$, i.e, $(A, B) \in R$, se $A \subset B$.

EXEMPLO 2: Ordem clássica "menor ou igual" nos reais (este é um caso especial em que todos os elementos são "comparáveis" entre si, o que se chama de **ordem total** ou **cadeia**).

EXEMPLO 3: Relação $a \preceq b$ se $a$ divide $b$ nos naturais.

CONTRA-EXEMPLO 1: Ordem "estritamente menor" nos reais não é reflexiva, pois não tenho $a < a$.

CONTRA-EXEMPLO 2: Divisibilidade nos inteiros não é antissimétrica pois $-a$ divide $a$ e $a$ divide $-a$ mesmo que $a \neq -a$

# Conceitos iniciais

Se $X$ é um conjunto dotado de uma relação de ordem parcial $\preceq$, diz-se que $z \in X$ é o **máximo** de $X$ se $x \preceq z, \forall x \in X$. Se tal máximo existir, ele será único.

Se $X$ é um conjunto dotado de uma relação de ordem parcial $\preceq$, diz-se que $a \in X$ é o **mínimo** de $X$ se $a \preceq x, \forall x \in X$. Se tal máximo existir, ele será único.

EXEMPLO: Conjunto $D_{18} = \{1, 2, 3, 6, 9, 18\}$ de todos os números que dividem 18 tem o máximo 18 e mínimo 1.

CONTRA-EXEMPLO: Conjunto $\{2, 3, 6, 12, 18\}$ com relação de divisibilidade não tem nem máximo nem mínimo.

# Conceitos iniciais

Seja $X$ um conjunto dotado da ordem $\preceq$ e $A \subset X$. Se existe um elemento $t \in X$ tal que $a \preceq t, \forall a \in A$, então diz-se que $t$ é um **majorante** ou **limitante superior** de $A$.

Analogamente, se existe um elemento $h \in X$ tal que $h \preceq a, \forall a \in A$, então diz-se que $h$ é um **minorante** ou **limitante inferior** de $A$.

O mínimo do conjunto de majorantes de $A$, se existir, é chamado de **supremo** de A. Já o máximo do conjunto de minorantes de $A$, se existir, é chamado de **ínfimo** de A.

# Conceitos iniciais

EXEMPLO: Subconjunto aberto $(0, 1)$ de $\mathbb{R}$ com relação $\leq$ tem como majorante qualquer $x \geq 1$ e como minorante qualquer $x \leq 0$. O supremo é 1 e o ínfimo é 0.

CONTRA-EXEMPLO: Seja $D_{36} = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$ e o subconjunto $A = \{2, 3\}$. $A$ tem como majorantes os elementos $6, 12, 18, 36$ e o supremo é 6. Já o minorante e também ínfimo é 1.

# Outline

# Reticulados

Um **reticulado** é uma estrutura $(L, \preceq)$ em que $L$ é um conjunto parcialmente ordenado e $\preceq$ uma relação de ordem parcial tal que para quaisquer $a, b \in L$ o conjunto $\{a, b\}$ possui supremo e ínfimo.

EXEMPLO 1: Conjunto de subconjuntos de $X$ ordenado pela relação "subconjunto de". Para qualquer par de conjuntos, o supremo é dado pela união e o ínfimo pela intersecção.

EXEMPLO 2: Inteiros positivos com relação usual $\leq$. Supremo é $\max\{a, b\}$ e ínfimo $\min\{a, b\}$.

EXEMPLO 3: $\{1, 2, 3, 6\}$ ordenado por divisibilidade. O supremo de $\{a, b\}$ é o mínimo múltiplo comum de $a$ e $b$ e o ínfimo é máximo divisor comum de $a$ e $b$.

# Reticulados

CONTRA-EXEMPLO 1: Conjunto $\{1, 2, 3\}$ não é reticulado pois $\{2, 3\}$ não possui sequer majorantes.

CONTRA-EXEMPLO 2: $\{1, 2, 3, 12, 18, 36\}$ por divisibilidade. O par $\{2, 3\}$ possui os majorantes $\{12, 18, 36\}$ mas 12 e 18 não são comparáveis e assim não há supremo. Similarmente, o par $\{12, 18\}$ tem os minorantes $\{1, 2, 3\}$ mas não tem ínfimo.

# Reticulados

Um reticulado é dito ser **limitado superiormente** se possuir um **máximo**, isto é, um elemento $\omega \in C$ tal que $x \preceq \omega, \forall x \in C$.

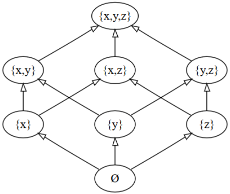
Um reticulado é dito ser **limitado inferiormente** se possuir um **mínimo**, isto é, um elemento $\alpha \in C$ tal que $\alpha \preceq x, \forall x \in C$.

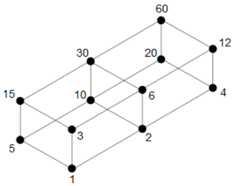
Um **reticulado completo** é aquele em que todo subconjunto seu não-vazio possui um supremo e um ínfimo em relação à ordem $\preceq$.

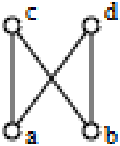
# Reticulados

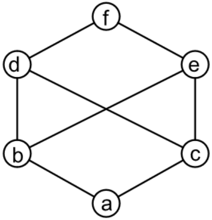
Representação visual amplamente usada é o **Diagrama de Hasse**. Os dois primeiros são reticulados (relações “subconjunto de” e “divide”).

No 3º, o par $\{c, d\}$ não possui sequer majorante e muito menos um supremo. No 4º, o par $\{b, c\}$ possui majorantes $d, e, f$ mas não um supremo.



# Outline

# Álgebras Universais - Conceitos iniciais

Sejam dois conjuntos não-vazios $C$ e $I$.

Uma função $f : C \times I \to C$ é chamada de **operação** sobre $C$.

Se $I$ é finito, a função $f : C \times I \to C$ é dita ser uma **função (operação) finitária** sobre $C$.

Em particular, uma função $f : C^n \to C$, para $n \in \mathbb{N}$, é chamada de **função** $n$**-ária**. Em específico, se $n = 1$ ou $n = 2$ temos uma **função binária** ou **unária**, respectivamente.

# Álgebras Universais - Conceitos iniciais

Um subconjunto $R \subset C \times I$ é chamado de **relação** sobre $C$. Se $R \subset C^n$ temos uma relação $n$-ária.

Seja $C$ um conjunto, $\mathfrak{F}$ uma coleção de operações sobre $C$ e $\mathfrak{R}$ uma coleção de relações sobre $C$. A tripla $< C, \mathfrak{F}, \mathfrak{R} >$ é chamada de **estrutura** sobre $C$.

.

# Álgebras Universais

Uma **álgebra universal** é composta por um conjunto $C$ e uma coleção $\mathfrak{F}$ (não necessariamente finita) de funções <u>finitárias</u> sobre $C$. Representa-se por $< C, \mathfrak{F} >$.

# Álgebras Universais

EXEMPLOS:

$C = \mathbb{R}$, $\mathfrak{F} = \{s, m\}$, em que $s$ e $m$ são funções binárias definidas por $s : \mathbb{R}^2 \to \mathbb{R}, s(x, y) = x + y$ e $m : \mathbb{R}^2 \to \mathbb{R}, m(x, y) = x \cdot y$

$C = Mat(\mathbb{C}, n)$ (conjunto das matrizes complexas de ordem $n \times n, n \in \mathbb{N}$), $\mathfrak{F} = \{s, m\}$, em que $s$ e $m$ são funções binárias definidas por $s : C^2 \to C, s(A, B) = A + B$ e $m : C^2 \to C, m(A, B) = A \cdot B$

$C = Mat(\mathbb{C}, m, n)$ (conjunto das matrizes complexas de ordem $m \times n, m, n \in \mathbb{N}$), $\mathfrak{F} = \{c, s, t\}$, em que $c$ é a função unária definida por $c : C \to C, c(A) = \overline{A}$ (matriz complexo-conjugada de $A$), $s$ é a função binária dada por $s : C^2 \to C, s(A, B) = A + B$ e $t$ é uma função 3-ária expressa por $t : C^3 \to C, t(A, B, C) = AB^T C$ ($B^T$ denota a transposta de $B$).

# Outline

# Reticulados como Estruturas Algébricas

Um **reticulado** pode também ser visto como uma álgebra universal composta por um conjunto não-vazio $C$ e duas funções binárias $\wedge$ e $\vee$ (lê-se "e" e "ou", respectivamente), satisfazendo as seguintes propriedades para quaisquer $a, b, c \in C$ (notação mesofixa):

1. Idempotência:
$$a \wedge a = a, \qquad a \vee a = a.$$
2. Comutatividade:
$$a \wedge b = b \wedge a, \qquad a \vee b = b \vee a.$$
3. Associatividade:
$$a \wedge (b \wedge c) = (a \wedge b) \wedge c \qquad a \vee (b \vee c) = (a \vee b) \vee c.$$
4. Absorvência (Amalgamento):
$$a \wedge (a \vee b) = a, \qquad a \vee (a \wedge b) = a.$$

# Reticulados como Estruturas Algébricas

EXEMPLO 1: Seja $C = \mathbb{P}(B)$, para algum conjunto não-vazio $B$, e para todo $a, b \subset B$ definimos $a \wedge b = a \cap b, a \vee b = a \cup b$.

EXEMPLO 2: Seja $C = \mathbb{R}$ e as seguintes funções binárias definidas para todo $a, b \in \mathbb{R}$: $a \wedge b := \min\{a, b\}$ e $a \vee b := \max\{a, b\}$.

# Reticulados como Estruturas Algébricas

**Lema**

Seja $C$ um conjunto não-vazio compondo um reticulado com as operações binárias $\wedge$ e $\vee$. Para $x, y \in C$ a igualdade $x = x \wedge y$ é satisfeita se e somente se $y = x \vee y$.

O Lema acima nos permite induzir uma ordem parcial a partir de um reticulado em $C$. Dizemos que $x \preceq y$ se e somente se $x = x \wedge y$ (ou equivalentemente pelo Lema $y = x \vee y$).

Note como as operações $\cap$ e $\cup$ no Exemplo 1 induzem a relação parcial "subconjunto de" e as operações max e min no Exemplo 2 induzem a relação $\leq$.

# Outline

# Outras estruturas algébricas - Magma

Ummagma (**grupoide**) é um conjunto não-vazio $N$ dotado de uma operação binária $N \times N \to N$ denotada $\cdot$ (produto) e satisfazendo a seguinte propriedade:

1. Fechamento: Para quaisquer $a, b \in N$:

$$(a \cdot b) \in N.$$

EXEMPLO 1: Soma nos reais

EXEMPLO 2: Multiplicação de matrizes reais

CONTRA-EXEMPLO 1: Soma nos reais excluindo o zero $(a + (-a) = 0)$

CONTRA-EXEMPLO 2: Conjunto de funções complexas com produto interno em um intervalo fechado (resultado é um número)

Todas as estruturas a seguir satisfazem o fechamento.

# Outras estruturas algébricas - Semi-grupo

Um **semi-grupo** é um conjunto não-vazio $S$ dotado de uma operação binária $S \times S \to S$ denotada $\cdot$ (produto) e satisfazendo a seguinte propriedade:

1. Associatividade: Para quaisquer $a, b, c \in S$:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

EXEMPLO 1: Conjunto dos naturais positivos ($\{1, 2, 3, \ldots\}$) formam semi-grupo na operação de soma.

EXEMPLO 2: Multiplicação de matrizes reais.

CONTRA-EXEMPLO 1: Reais com operação $-$ $((a - b) - c \neq a - (b - c))$.

CONTRA-EXEMPLO 2: Reais com operação média $a \oplus b = (a + b)/2$.

# Outras estruturas algébricas - Monoide

Um **monoide** é um conjunto não-vazio $M$ dotado de uma operação binária $M \times M \to M$ denotada $\cdot$ (produto) e satisfazendo as seguintes propriedades:

1. Associatividade: Para quaisquer $a, b, c \in M$:
$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$
2. Elemento neutro (identidade): Existe (e é único) um elemento $e \in M$ tal que
$$g \cdot e = e \cdot g = g, \forall g \in M.$$

EXEMPLO 1: Conjunto $Mat(\mathbb{C}, n)$ das matrizes complexas $n \times n$ sob o produto usual de matrizes é um monoide.

EXEMPLO 2: $\mathbb{R}$ sob multiplicação formam um monoide.

# Outras estruturas algébricas - Monoide

CONTRA-EXEMPLO 1: $\{x \in \mathbb{R}, x > 0\}$ forma semigrupo em relação à soma, mas não um monoide pois o elemento neutro (0) não está no conjunto.

CONTRA-EXEMPLO 2: Conjunto de *srings* não vazias sob a operação de concatenação (elemento identidade seria exatamente a *string* vazia).

## Outras estruturas algébricas - Grupo

Um **grupo** é um conjunto não-vazio $G$ dotado de uma operação binária $G \times G \to G$ denotada $\cdot$ (produto) e uma operação unária $G \to G$ denotada $^{-1}$ (inversa) e satisfazendo as seguintes propriedades:

1. Associatividade: Para quaisquer $a, b, c \in G$:
$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$
2. Elemento neutro: Existe (e é único) um elemento $e \in G$ tal que
$$g \cdot e = e \cdot g = g, \forall g \in G.$$
3. Inversa: Para cada $g \in G$ existe e é único um elemento $h \in G$ tal que
$$g \cdot h = h \cdot g = e.$$
$h$ é chamado de inversa de $g$ e denotado $g^{-1}$.

Se o grupo também satisfizer a comutatividade, é chamado de **abeliano**.

# Outras estruturas algébricas - Grupo

EXEMPLOS:

Conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são grupos abelianos em relação à soma usual. Tais grupos costumam ser denotados respectivamente $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ e $(\mathbb{C}, +)$.

Conjuntos $\mathbb{Q}\backslash\{0\} = \{r \in \mathbb{Q}, r \neq 0\}$, $\mathbb{R}\backslash\{0\} = \{x \in \mathbb{R}, x \neq 0\}$ e $\mathbb{C}\backslash\{0\} = \{z \in \mathbb{C}, z \neq 0\}$ são grupos abelianos em relação à multiplicação usual. Tais grupos costumam ser denotados respectivamente $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ e $(\mathbb{C}, \cdot)$.

Conjunto $GL(\mathbb{R}, n)$ de todas as matrizes reais $n \times n, n > 1$ com determinante não-nulo (inversíveis) formam um grupo não-abeliano.

# Outras estruturas algébricas - Grupo

CONTRA-EXEMPLOS:

Conjunto $\mathbb{R}_+ = \{x \in \mathbb{R}, x \geq 0\}$ com a operação de soma não possui inversa.

Conjunto $Mat(Mat(\mathbb{C}, n))$ das matrizes complexas $n \times n$ com a operação de multiplicação de matrizes não tem inversa garantida.

# Outras estruturas algébricas - Corpo

Um **corpo** é um conjunto não-vazio $\mathbb{F}$ dotado de duas operações binárias, $+$ (soma) e $\cdot$ (produto), de modo que a soma satisfaça:

1. Comutatividade: Para quaisquer $a, b \in \mathbb{F}$:
$$a + b = b + a.$$
2. Associatividade: Para quaisquer $a, b, c \in \mathbb{F}$:
$$(a + b) + c = a + (b + c).$$
3. Elemento neutro: Existe (e é único) um elemento $0 \in \mathbb{F}$, chamado **elemento nulo**, tal que
$$a + 0 = 0 + a, \forall a \in \mathbb{F}.$$
4. Inversa: Para cada $a \in \mathbb{F}$ existe e é único um elemento $b \in \mathbb{F}$ tal que
$$a + b = 0.$$
Denota-se $b$ por $-a$.

# Outras estruturas algébricas - Corpo

Já o produto deve satisfazer:

1. Comutatividade: Para quaisquer $a, b \in \mathbb{F}$:
$$a \cdot b = b \cdot a.$$
2. Associatividade: Para quaisquer $a, b, c \in \mathbb{F}$:
$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$
3. Elemento neutro: Existe (e é único) um elemento $1 \in \mathbb{F}$, chamado **unidade**, tal que
$$a \cdot 1 = 1 \cdot a, \forall a \in \mathbb{F}.$$
4. Inversa: Para cada $a \in \mathbb{F}, a \neq 0$ existe e é único um elemento $b \in \mathbb{F}$ tal que
$$a \cdot b = 1.$$
Denota-se $b$ por $a^{-1}$.

# Outras estruturas algébricas - Corpo

Finalmente, o produto deve ser distributivo em relação à adição, ou seja, para todo $a, b, c \in \mathbb{F}$:

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

# Outras estruturas algébricas - Corpo

EXEMPLOS:

$\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ com soma e produto clássicas.

Conjunto $\mathbb{Q}(\sqrt{2})$ contendo números da forma $a + b\sqrt{2}$, com $a$ e $b$ racionais e as operações usuais. Em geral, para qualquer $p$ primo o conjunto $\mathbb{Q}(\sqrt{p})$ forma um corpo.

CONTRA-EXEMPLOS:

Matrizes $n \times n, n \geq 2$ com adição e produto de matrizes (produto não-comutativo).

Inteiros módulo 4: $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ com soma e produto usual (2 por exemplo não possui inverso multiplicativo). Em geral, $\mathbb{Z}_n$ só é corpo para $p$ primo.

# Outras estruturas algébricas - Anel

Um **anel** é um conjunto não-vazio $A$ dotado de duas operações binárias, $+$ (soma) e $\cdot$ (produto), de modo que a soma satisfaça os mesmos requisitos de um corpo:

1. Comutatividade: Para quaisquer $a, b \in \mathbb{F}$:
$$a + b = b + a.$$
2. Associatividade: Para quaisquer $a, b, c \in \mathbb{F}$:
$$(a + b) + c = a + (b + c).$$
3. Elemento neutro: Existe (e é único) um elemento $0 \in \mathbb{F}$, chamado **elemento nulo**, tal que
$$a + 0 = 0 + a, \forall a \in \mathbb{F}.$$
4. Inversa: Para cada $a \in \mathbb{F}$ existe e é único um elemento $b \in \mathbb{F}$ tal que
$$a + b = 0.$$
Denota-se $b$ por $-a$.

# Outras estruturas algébricas - Anel

Já em relação ao produto ele se comporta como um semi-grupo (não precisa ser comutativo nem ter inversa) devendo apenas satisfazer:

1. Associatividade: Para quaisquer $a, b, c \in \mathbb{F}$:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

Finalmente, o produto deve ser distributivo em relação à adição, ou seja, para todo $a, b, c \in \mathbb{F}$:

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

# Outras estruturas algébricas - Anel

EXEMPLOS:
Matrizes reais $n \times n$ com a adição e multiplicação clássica de matrizes.

Inteiros módulo 4: $Z_4 = \{0, 1, 2, 3\}$ com adição e produto feito como de praxe mas com o resultado sendo o resto da divisão inteira por 4.

CONTRA-EXEMPLOS:
Números naturais (não incluindo zero) com adição e produto convencionais (não possui inverso aditivo).

Conjunto de funções com suporte limitado e com adição usual e produto definido pela convolução:

$$(f * g)(x) = \int_{-\infty}^{\infty} f(y)g(x-y)dy.$$

O único elemento que funcionaria como identidade do produto seria o $\delta$ de Dirac, mas este não é propriamente uma função.

# Outras estruturas algébricas - Semi-anel

Um semi-anel é idêntico a um anel exceto pelo fato de que não se exige a definição de uma inversa aditiva.

EXEMPLOS:

Todo anel é por definição também um semi-anel. Exemplos particulares de semi-aneis são, respectivamente, o conjunto dos naturais (incluindo 0), bem como dos reais não-negativos e racionais não-negativos, sob as operações clássicas de adição e multiplicação.

Matrizes $n \times n$ com entradas não negativas sob as operações convencionais de adição e multiplicação de matrizes (não necessariamente comutativo).

Em linguagens formais, denotamos um alfabeto de símbolos por $\Sigma$ e o conjunto de palavras possíveis por $\Sigma^*$. Um exemplo de semi-anel é uma linguagem formal (subconjunto de $\Sigma^*$) dotada de um produto definido pela concatenação de *strings* e uma adição definida pela união dos conjuntos de cada linguagem.

# Representação Esquemática

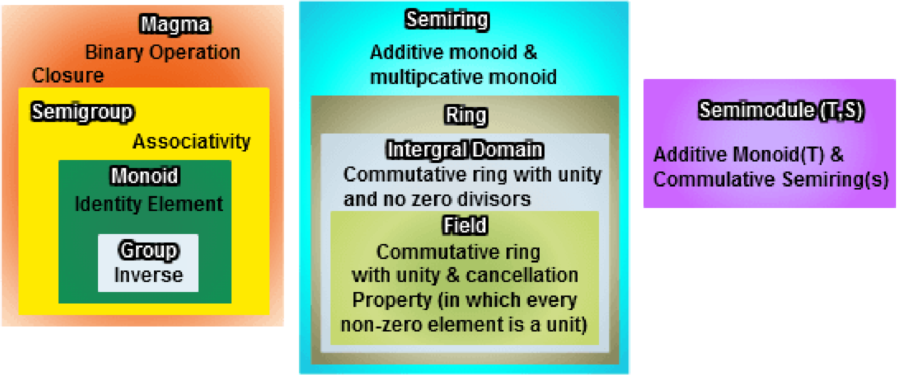



Figura: Fonte: mathcaptain.com