

Nota

p/ - para
qq - qualquer
tq - tal que
sse - se e só se (\Leftrightarrow)
então (\Rightarrow)

Máximo Divisor Comum

$$\begin{aligned}36 &= 2 \times 2 \times 3 \times 3 \\90 &= 2 \times 3 \times 3 \times 5 \\MDC(36, 90) &= 2 \times 3 \times 3 = 18\end{aligned}$$

Mínimo Múltiplo Comum

múltiplos de 6: 0, 6, 12, 18, 24, 30, ...
múltiplos de 4: 0, 4, 8, 12, 16, 20, 24, ...
MMC(6, 4) = 12 (pois é o menor múltiplo comum diferente de zero)

$$a \equiv b \pmod{n} \rightarrow a - b = kn$$

Uma função diz-se **injetiva** se p/ cada elemento $x \in X$, existe um único $y \in Y$ tq $f(x) = y$.

Uma função diz-se **sobrejetiva** se p/ cada elemento $y \in Y$, existe pelo menos um $x \in X$ tq $f(x) = y$.

Uma função diz-se **bijetiva** se for injetiva e sobrejetiva.

Associatividade: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

Uma operação \cdot é associativa quando p/ qq 3 elementos do conjunto/grupo se verifica regra acima

Comutatividade/Abeliano: $a \cdot b = b \cdot a$

Uma operação \cdot é comutativa quando p/ qq 2 elementos do conjunto/grupo se verifica a regra acima

Seja $(S, *)$ um grupóide.

Um elemento $0 \in S$ diz-se um **elemento zero/nulo** se $0 * a = 0 = a * 0$, $\forall a \in S$.

Um elemento $id \in S$ diz-se um **elemento neutro/identidade** se $id * a = a = a * id$, $\forall a \in S$.

Um elemento $a \in S$ diz-se um **elemento idempotente** se $a * a = a$. Um elemento neutro/nulo é um elemento idempotente. Num grupóide existe no máximo um elemento neutro - representado por 1_S .

Um grupóide diz-se **semigrupo** se a sua operação $*$ for associativa.

Seja S um semigrupo, $m, n \in \mathbb{N}$ e $a \in S$, então:

- $a^m a^n = a^{m+n}$ [$ma + na = (m+n)a$];
- $(a^m)^n = a^{mn}$ [$n(ma) = (nm)a$].

Um semigrupo que admita elemento neutro, diz-se um **monóide** ou **semigrupo com identidade**.

Seja $(S, *)$ um monóide.

Um elemento $a' \in S$ diz-se um elemento oposto de a se $a' * a = 1_S = a * a'$.

Um elemento $a \in S$, tem no máximo, um elemento oposto.

Oposto:

inverso de $a = a^{-1}$ [Linguagem Multiplicativa]
simétrico de $a = -a$ [Linguagem Aditiva]

A não ser que seja referido, trabalhamos com linguagem multiplicativa.

Princípio da Boa Ordenação: todo subconjunto não-vazio de \mathbb{N} possui um elemento mínimo (menor elemento).

TEORIA DE GRUPOS

Um Grupo é um monóide no qual todos elementos admitem um único elemento opostos.

G é grupo sse:

- 1) a operação binária é associativa
- 2) $\forall a \exists id \in G: a \cdot id = a = id \cdot a$
(se qualquer elemento de G admita um elemento identidade que pertença a G)
- 3) $\forall a \exists (a^{-1}) \in G: a \cdot (a^{-1}) = id = (a^{-1}) \cdot a$
(se para qualquer elemento de G haja um elemento oposto pertencente a G)

Seja G um grupo:

- > $id^{-1} = id$
- > $(x^m) \cdot (x^n) = x^{m+n}; (x^m)^n = x^{m \cdot n}$
- > $(a^{-1})^{-1} = a; (a \cdot b)^{-1} = (b^{-1}) \cdot (a^{-1}); (a_1 \dots a_n)^{-1} = (a_n^{-1}) \dots (a_1^{-1})$
- > são válidas as **leis de corte**: para $x, y, a \in G, a \cdot x = a \cdot y \Rightarrow x = y$

Existem semigrupos que não são grupos, nos quais se verifica as leis do corte – por ex.: $\mathbb{Z} \setminus \{0\}$, este monóide comutativo as leis do corte mas não é um grupo (pois os únicos elementos que admitem inverso são 1 e -1).

Também a igualdade $(xy)^n = x^n y^n (\forall x, y \in G \text{ e } n \in \mathbb{N})$ só se verifica sse G é abeliano.

Seja G um grupo, e S o seu subconjunto não vazio (=subgrupo, escrevemos $S < G$)

$S \subseteq G$ é $S < G$ sse:

- $S \neq \emptyset$ vazio (pois pelo menos a $id(G) \in S$)*
- $x, y \in S \Rightarrow xy \in S$
- $x \in S \Rightarrow x^{-1} \in S$

*se G é grupo e $S < G$ então o elemento neutro de S (1_S) é o mesmo que o de G (1_G). Pois por um lado temos que, $1_S * 1_S = 1_S$; por outro lado, como $1_S \in G$, temos que $1_S * 1_G = 1_S$. Logo pela lei do corte, $1_S * 1_S = 1_S * 1_G \Leftrightarrow 1_S = 1_G$

Sejam G um grupo e $S < G$. Então:

- para cada $s \in S$, o inverso de s em S é o mesmo que o inverso de s em G
- para $S_1, S_2 < G$ então $S_1 \cap S_2 < G$

Ordem do Grupo é o nº de elementos do grupo G, e representa-se por $|G|$

Ordem de um Elemento é o menor n.º natural p tq um elemento a pertencente a um grupo G dê $a^p = 1_G$ - representa-se por $o([a]_p)$ - dito de outra forma, $o(a) = k$ se: a) $a^k = 1_G$; b) $p \in \mathbb{N}, a^p = 1_G \Rightarrow k \leq p$

Seja G grupo e $a \in G$ um elemento de ordem finita f.

Então para qq $n \in \mathbb{N}$: $o(a^n) = \frac{f}{\text{mdc}(f, n)}$.

Se não existe nenhum $n \in \mathbb{N}$ tq $a^n = 1_G$ então diz-se que a tem ordem infinita e escrevemos $o(a) = \infty$.

Num grupo finito, a ordem de cada elemento divide a ordem do grupo.

Num grupo finito nenhum elemento tem ordem infinita.

Num grupo o elemento identidade é o único com ordem 1.

Sejam G um grupo e $a, b \in G$. Então, p/ qq inteiro positivo k: $(ab)^k = 1_G \Leftrightarrow (ba)^k = 1_G$.

Sejam G um grupo e $a \in G$, então: $o(a^{-1}) = o(a)$.

Se $(x, y) \in \mathbb{Z}_n \cdot \mathbb{Z}_m$ então $o((x, y)) = \text{mmc}(o(x), o(y))$.

Seja S um semigrupo finito que satisfaz as leis do corte, então S é um grupo.

Teorema de Lagrange: Seja G grupo finito e $H < G \Rightarrow |H|$ divide por $|G|$

Teorema de Cauchy: Seja G um grupo de ordem $n \in \mathbb{N}$ e p um primo divisor de n. Então, existe um elemento $a \in G$ tq $o(a) = p$.

Sejam G um grupo e $\emptyset \neq X \subseteq G$.

Chama-se **subgrupo de G gerado por X**, e representa-se por $\langle X \rangle$, ao menor subgrupo que contém X.

Se $X = \{a\}$, então escrevemos $\langle a \rangle$ para representar $\langle X \rangle$ e falamos no **subgrupo de G gerado por a**.

Sejam G e $a \in G$ um elemento com ordem infinita, então $\langle a \rangle$ tem nº infinito de elementos.

Se $G = \langle a \rangle$ tem ordem o, então p/ $1 \leq n \leq o - 1, a^n$ é gerador de G sse $\text{mdc}(n, o) = 1$.

Se por exemplo $G = \langle a \rangle$ tem ordem vinte, então, a^n é gerador de G sse $\text{mdc}(n, 20) = 1$, ou seja, sse $n \in \{1, 3, 7, 9, 11, 13, 17, 19\}$. Logo G tem 8 geradores.

Seja G um grupo abeliano, então $H < G$ é **subgrupo normal/invariante** de G (escreve-se $H \triangleleft G$)
Ou seja $\forall x \in G, xH = Hx$

Seja G um grupo abeliano, então qq subgrupo H de G é normal em G .

Seja G grupo e $H < G$ e $H' \triangleleft G$. Então, $HH' \triangleleft G$. Também se $H' \subseteq H$, então $H' \triangleleft H$.

Seja G grupo e $H \triangleleft G$, então, ao grupo G/H chama-se **grupo quociente** (que é abeliano)

Demonstração: Sejam $x, y \in G$, então, $xHyH = xyHH = xyH$

2º Teorema do Isomorfismo - Sejam G grupo e $H, T < G$ tq $T \triangleleft G$. Então $(HT)/T \cong H/(H \cap T)$.

Grupo Cíclico: $\exists a \in G: G = \langle a \rangle$, i.e, se existe $a \in G$ tq - $(\forall x \in G)(\exists n \in \mathbb{Z}) x = a^n$

Qualquer subgrupo de um grupo cíclico é cíclico.

Grupo Quociente de um grupo cíclico é cíclico.

Grupo Quociente de um grupo que não é cíclico pode ser cíclico.

Todo grupo cíclico é abeliano (o recíproco não é verdadeiro).

Dois grupos cíclicos são isomorfos sse tiverem a mesma ordem.

G cíclico ordem p (sendo p um nº primo), então, $G \cong \mathbb{Z}_p$ (G é isomorfo a \mathbb{Z}_p).

Uma aplicação $\Psi: G_n \rightarrow G_m$ diz-se um **morfismo**, ou **homomorfismo**, se: $\forall x, y \in G_n, \Psi(xy) = \Psi(x)\Psi(y)$

Um morfismo diz-se um **epimorfismo** se for uma aplicação sobrejetiva, isto é se: $\forall y \exists x, Y(x) = y$

Um morfismo diz-se um **monomorfismo** se for uma aplicação injetiva, isto é sse: $\forall a, b \in X \Rightarrow Y(a) \neq Y(b)$

Um morfismo diz-se **isomorfismo** se for uma aplicação bijetiva (ou seja, sobrejetiva e injetiva)

Um morfismo de um grupo nele mesmo diz-se **endomorfismo** (**automorfismo** se for bijetivo)

Conjunto automorfismo é um grupo p/ a composição usual de funções.

Seja $\psi: G_n \rightarrow G_m$ um morfismo de grupos

Chama-se **núcleo** (ou kernel) de ψ , e representa-se por **Nuc ψ** (ou $\ker \psi$), ao subconjunto de G_n :

$$\text{Nuc } \psi = \{x \in G_n \mid \psi(x) = 1_{G_m}\}$$

Sejam G um grupo e $H \triangleleft G$, então:

$$\begin{aligned} \pi: G &\rightarrow G/H \\ x &\mapsto xH \end{aligned}$$

é um epimorfismo (ao qual se chama epimorfismo canónico) tq **Nuc π** = H .

Sejam G_n e G_m dois grupos; se $\Psi: G_n \rightarrow G_m$ é um momorfismo, então: $\Psi(1_{G_n}) = 1_{G_m}$.

Sejam G_n e G_m dois grupos e $\Psi: G_n \rightarrow G_m$ um momorfismo, então: $[\Psi(x)]^{-1} = \Psi(x^{-1})$.

Sejam G_n e G_m dois grupos, $H \subseteq G_n$ e $\psi: G_n \rightarrow G_m$ um morfismo, então: $H < G_n \Rightarrow \psi(H) < G_m$.

Seja $\psi: G_n \rightarrow G_m$ um morfismo de grupos. Se ψ é um monomorfismo então $G_n \cong \psi(G_n)$.

Sejam G_n e G_m dois grupos, $H \subseteq G_n$ e $\psi: G_n \rightarrow G_m$ um epimorfismo. Então, $H \triangleleft G_n \Rightarrow \psi(H) \triangleleft G_m$.

Seja $\psi: G_n \rightarrow G_m$ um morfismo de grupos. Então, ψ é um monomorfismo se e só se $\text{Nuc } \psi = \{1_{G_n}\}$.

Seja $\psi: G_n \rightarrow G_m$ um morfismo de grupos definido por $\psi(x) = 1_{G_m} (\forall x \in G_n)$. Então ψ é morfismo de grupos **nulo**.

Teorema Fundamental do Homomorfismo:

Seja $\theta: G \rightarrow G'$ um morfismo de grupos. Então, $\text{Im } \theta \cong G/\text{Nuc } \theta$.

Teorema de representação de Cayley:

Todo o grupo é isomorfo a um grupo de permutações.

TEORIA DE ANÉIS

Seja A um conjunto não vazio e duas operações binárias, que representamos por $+$ e \cdot , nele definidas. O triplo $(A, +, \cdot)$ diz-se um **anel** se:

- 1) $(A, +)$ é um grupo comutativo (também chamado **módulo**)
- 2) (A, \cdot) é um semigrupo
- 3) A operação \cdot é distributiva em relação à operação $+$
(i.e., para todos $a, b, c \in A$, $a \cdot (b+c) = a \cdot b + a \cdot c$ e $(b+c) \cdot a = b \cdot a + c \cdot a$)

O anel A diz-se comutativo se a multiplicação for comutativa.

Seja $(A, +, \cdot)$ um anel:

- > Ao elemento neutro do grupo chamamos **zero do anel** e representamos por 0_A
- > Quando existe, ao elemento neutro do semigrupo chamamos **identidade do anel** e representamos por 1_A
- > No caso de o anel ter identidade, podem existir elementos que admitem elemento oposto p/ multiplicação
- > para todo $x \in A$, $0_A x = x 0_A = 0_A$
- > se $a+a=a$ e $a \cdot a=a$, é um anel comutativo com identidade, chamamos A um **anel nulo**
- > sejam $x, y \in A$, então, $(-x)y = x(-y) = -xy$ e $(-x)(-y) = xy$

Sejam $a, b \in A$ e $m, n \in \mathbb{Z}$, então:

- $(m+n)a = ma+na$
- $n(ma) = (nm)a$
- $n(a+b) = na+nb$
- $n(ab) = (na)b = a(nb)$
- $(a^n)^m = a^{nm}$
- $a^n a^m = a^{n+m}$

Propriedade Distributiva Generalizada

Sejam A um anel, $n \in \mathbb{N}$ e $a, b_1, b_2, \dots, b_n \in A$. Então:

- 1) $a(b_1+b_2+\dots+b_n) = ab_1+ab_2+\dots+ab_n$
- 2) $(b_1+b_2+\dots+b_n)a = b_1a+b_2a+\dots+b_na$

Seja A um anel com identidade 1_A , um elemento $a \in A$ diz-se uma **unidade** se admite inverso em A .

Representa-se por U_A o conjunto das unidades de um anel com identidade.

Seja A um anel, um elemento $a \in A$ diz-se **simplificável** se, para todos $x, y \in A$: $xa=ya$ ou $ax=ay \Rightarrow x=y$
Num anel A , toda a unidade é simplificável, mas nem todo o elemento simplificável é uma unidade.

Técnicamente são as leis do corte.

Seja A um anel, $a \in A$ diz-se um **divisor de zero** se existe $b \in A \setminus \{0_A\}$ tq: $ab=0_A$ ou $ba=0_A$

No anel $(\mathbb{Z}_n, +, \cdot)$, os divisores de zero são os elementos $[x]_n$, onde $\text{mdc}(x, n) \neq 1$

Para um anel $(A, +, \cdot)$, $n \in \mathbb{N}$, os elementos $[x]_n$ com $\text{mdc}(x, n)=1$ são as unidades do anel.

Por estas duas propriedades podemos concluir que uma unidade não pode ser um divisor de zero.

Seja A um anel:

- 1) se $na=0_A, \forall a \in A \Rightarrow n=0$, A diz-se anel de **caraterística 0** e escreve-se $c(A)=0$;
- 2) se $(\exists x \in \mathbb{Z} \setminus \{0\})(\forall a \in A) xa=0_A$, A diz-se anel de **caraterística k** onde k escreve-se $c(A)=k$

Sejam $A \neq \{0_A\}$ um anel com identidade 1_A e $n \in \mathbb{N}$. Então, $c(A)=n \Leftrightarrow o(1_A)=n$.

$*k = \min \{n \in \mathbb{N} : na = 0_A \forall a \in A\}$

Seja A um anel e a um elemento de A : $c(A)=k$; $o(a)=x$; então $\forall b \in A - kb=0_A \Rightarrow x|k$.

Domínio de Integridade - um anel comutativo com identidade tq 0_A é o único divisor de zero

Se A é um domínio de integridade, então, $A \neq \{0_A\}$.

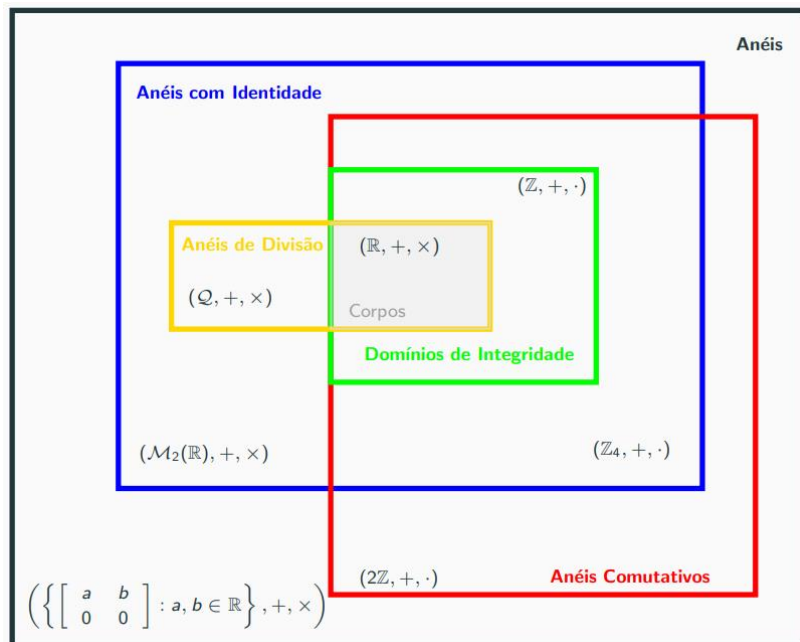
Seja A um anel comutativo com identidade. Então, as seguintes afirmações são equivalentes:

- A é domínio de integridade;
- $A \setminus \{0_A\} \neq \emptyset$ e todo o elemento de $A \setminus \{0_A\}$ é simplificável;
- $A \setminus \{0_A\} \neq \emptyset$ e $A \setminus \{0_A\}$ é subsemigrupo de A relativamente ao produto;
- $A \setminus \{0_A\} \neq \emptyset$ e, se as equações $ax=b$ e $xa=b$ ($a \neq 0_A$) tiverem solução, então, a solução é única.

Um anel A diz-se um **anel de divisão** se $(A \setminus \{0_A\}, \cdot)$ é um grupo.

Um anel de divisão comutativo diz-se um **corpo**.

Resulta da definição que qq corpo é um domínio de integridade (o recíproco não é verdadeiro).



Sejam A um anel e $A' \subseteq A$. Então, A' é **subanel** de A sse:

- 1) $A' \neq \emptyset$
- 2) $x, y \in A' \Rightarrow x - y \in A'$
- 3) $x, y \in A' \Rightarrow xy \in A'$

Sejam A um domínio de integridade e $A' \subseteq A$.

Então, A' é **subdomínio** de integridade de A sse:

- 1) $1_A \in A'$
- 2) $x, y \in A' \Rightarrow x - y \in A'$
- 3) $x, y \in A' \Rightarrow xy \in A'$

Sejam A um anel de divisão (respetivamente, **corpo**) e $A' \subseteq A$.

Então, A' é subanel de divisão (respetivamente, **subcorpo**) de A sse:

- 1) $A' \neq \emptyset$
- 2) $x, y \in A' \Rightarrow x - y \in A'$
- 3) $x, y \in A' \setminus \{0_A\} \Rightarrow xy^{-1} \in A' \setminus \{0_A\}$

Seja A um anel, I é **ideal** de A se:

- 1) $(I, +) < (A, +)$
- 2) $\forall x \in A \forall i \in I, xi, ix \in I \quad (I \subseteq A, I \neq \emptyset)$

Todo ideal de um anel A é um subanel de A

Ideal próprio:

- $I \subsetneq A$
- $I \subseteq A$ mas $I \neq A$

Seja A um anel comutativo com identidade, um ideal I diz-se **ideal maximal** de A se não existe K ideal de A tq: $I \subsetneq K \subsetneq A$

Se existir $K \subseteq A$ tq $I \subsetneq K$ então $I \neq K$

Se I e J são ideais maximais distintos de um anel comutativo com identidade A , então $A = I + J$

Seja A um anel comutativo com identidade e I um ideal de A .

Então, são equivalentes as seguintes afirmações:

- I é maximal
- A/I é corpo

$$I=A \text{ se } 1_A \in I$$

Sejam A e A' dois anéis.

Uma aplicação $\varphi:A \rightarrow A'$ diz-se um **morfismo** (ou homomorfismo) de anéis se satisfaz as seguintes condições:

- 1) $(\forall a, b \in A) \varphi(a+b) = \varphi(a) + \varphi(b)$
- 2) $(\forall a, b \in A) \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

Um morfismo diz-se um **monomorfismo** se for injetivo.

Enquanto que um morfismo sobrejetivo diz-se **epimorfismo**, e **isomorfismo** caso for bijetivo.

Um morfismo diz-se um **endomorfismo** se $A=A'$. Um endomorfismo bijetivo diz-se um **automorfismo**.

Sejam A e A' dois anéis e $\varphi: A \rightarrow A'$ um morfismo. Então, $\varphi(0_A) = 0_{A'}$

Sejam A e A' dois anéis e $\varphi: A \rightarrow A'$ um morfismo. Então, $(\forall a \in A) \varphi(-a) = -\varphi(a)$

Sejam A e A' dois anéis e $\varphi: A \rightarrow A'$ um morfismo. Então, $(\forall a \in A) (\forall k \in \mathbb{Z}) \varphi(ka) = k\varphi(a)$

Sejam $\varphi:A \rightarrow A'$ um morfismo de anéis e B um subanel de A . Então, $\varphi(B)$ é um subanel de A'

Sejam $\varphi:A \rightarrow A'$ um epimorfismo de anéis e I um ideal de A . Então, $\varphi(I)$ é um ideal de A'

Seja $\varphi:A \rightarrow A'$ um morfismo não nulo de anéis, se A é um corpo, então, $\varphi(A)$ é um corpo

Seja $\varphi:A \rightarrow A'$ um morfismo de anéis, então $A/\text{Nuc } \varphi$ é isomorfo a $\varphi(A)$

Permutações

Seja A um conjunto, uma permutação de A é uma aplicação bijetiva de A em A

Se A é um conjunto de $n \in \mathbb{N}$, sabemos que podemos definir $n!$ Permutações de A distintas

Ordem de σ só pode ser ou:

- comprimento do ciclo
- MMC do comprimento dos ciclos disjuntos

$$|\langle \sigma \rangle| = o(\sigma) = x$$

Você está visualizando a tela de Catarina Faustino Visualizar Opções

Ex 1

(a) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 6 & 3 & 7 & 5 & 1 \end{pmatrix}$

$\sigma = (\underline{1 \ 2 \ 4 \ 3 \ 6 \ 5 \ 7})$

$\theta(\sigma) = 7$

$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 6 & 7 & 5 \end{pmatrix}$

$\tau = (\underline{1 \ 2 \ 3 \ 4})(\underline{5 \ 6 \ 7})$

$\theta(\tau) = \text{mmc}(4, 3) = 12$

$\tau = (\underline{1 \ 2 \ 3 \ 4})(\underline{2 \ 3 \ 6 \ 5 \ 7})$

$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 6 & 7 & 5 \end{pmatrix}$

$\tau = (\underline{1 \ 2 \ 3 \ 4})(\underline{3 \ 6 \ 5 \ 7})$

Seja $\sigma \in S_8$ tal que $\theta(\sigma) = 5$

Por uma Proposição

$$|\langle \sigma \rangle| = \theta(\sigma) = 5$$

e) $\varphi: A \rightarrow A'$ morf. de anéis

I ideal de A $(I \subseteq A, I \neq \emptyset)$

(F)

(i) $(I, +) \leq (A, +)$

(ii) $\forall x \in A \forall i \in I, xi, ix \in I$
 $\varphi(I)$

Anel $\begin{cases} c(A) = 0 \\ c(A) = n \in \mathbb{N} \end{cases}$

$c(A) = n$ se $n \in \mathbb{N}$ for o menor natural tal que

$$n \cdot a = 0_A, \forall a \in A$$

$c(A) = 0$ se não existir qualquer natural n tq

$$n a = 0_A, \forall a \in A$$

(c) $a, b \in A$

$$\begin{aligned} (a+b)(a-b) &= a \cdot a + a \cdot (-b) + b \cdot a + b \cdot (-b) \\ &= \underline{a^2} - \underline{ab} + \underline{ba} - \underline{b^2} \end{aligned}$$

se A for abeliano (F)

(d) Dom int: A anel comutativo tal que 0_A é o único divisor de zero

$a \in A$ é divisor de zero se existe $b \in A \setminus \{0_A\}$ tal que

$$ab = 0_A \text{ ou } ba = 0_A$$

Prop: A anel: $A \neq \{0_A\}, 1_A \in A$ então $c(A) = n \in \mathbb{N} \Leftrightarrow \theta(1_A) = n$

(h) Sejam I, J ideais próprios de A .

Suponhamos que $I \cap J$ é um ideal maximal de A .

? $I = J$?

É claro que

$$I \cap J \subseteq I \quad (1)$$

$$I \cap J \subseteq J \quad (2)$$

$$(1) + I \cap J \text{ maximal} \Rightarrow I = I \cap J$$

$$(2) + I \cap J \text{ maximal} \Rightarrow J = I \cap J$$

$$\text{logo } I = I \cap J = J$$

Ideal próprio: $I \subsetneq A$

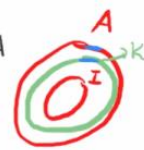
$I \subseteq A$ mas $I \neq A$



I é ideal maximal se não existe K ideal de A tq

$$I \subsetneq K \subsetneq A$$

se existir $K \subseteq A$ tq $I \subsetneq K$ então $I = K$



$$I = A \text{ se } 1_A \in I$$

(V)

$u(A \cdot)$