Nota

p/ - para
qq - qualquer
tq - tal que
i.e. - isto é
sse - se e só se (⇔)
então (⇒)

Máximo Divisor Comum

36 = 2 x **2** x **3** x **3**
90 = **2** x **3** x **3** x 5
MDC(36,90) = 2x3x3 = 18

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)

$$\mathbf{a \equiv b\,(mod\ n) \longrightarrow a - b = kn}$$

Seja $\boldsymbol{f}$ uma função de domínio **X** e contradomínio **Y**, $\boldsymbol{f: X \to Y}$.

A função $\boldsymbol{f}$ diz-se **injetiva** se p/ cada elemento $x \in X$, existe um <u>único</u> $y \in Y$ tq $f(x) = y$.

A função $\boldsymbol{f}$ diz-se **sobrejetiva** se p/ cada elemento $y \in Y$, existe <u>pelo menos</u> um $x \in X$ tq $f(x) = y$.

A função $\boldsymbol{f}$ diz-se **bijetiva** se for injetiva e sobrejetiva.

Associatividade: (a•b)•c = a•(b•c)
Uma operação • é associativa quando p/ qq 3 elementos do conjunto/grupo se verifica regra acima

Comutatividade/Abeliano: a•b = b•a
Uma operação • 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 $\mathbf{1}_S$.

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:

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

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 $a' * a = \mathbf{1}_S = a * a'$.
Um elemento $a \in S$, tem no máxmio, 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).

$\mathbb{Z}_n = \{0, \dots, n-1\}$

Seje • uma operação comutativa, $(x \bullet y)^2 = x^2 \bullet y^2$.

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) $\forall a \exists id \in G$: $a \bullet id = a = id \bullet a$
(se qualquer elemento de G admita um elemento identidade que pertença a G)

3) $\forall a \exists (a^{-1}) \in G$: $a \bullet (a^{-1}) = id = (a^{-1}) \bullet a$
(se para qualquer elemento de G haja um elemento oposto pertencente a G)

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

Existem semigrupos que não são grupos, nos quais se verifica as leis do corte – por ex.: $\mathbb{Z} \backslash \{0\}$, 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 $(xy)^n = x^n y^n$ $(\forall x, y \in G$ 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⊆G é S<G sse:
- S ≠ ∅ vazio (pois pelo menos a id(G)∈S)*
- x,y∈S ⟹ xy∈S
- x∈S ⟹ x^{-1}∈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∈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∈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 <u>nº de elementos do grupo</u> G, e representa-se por **|G|**

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

Seja G grupo e a ∈ G um elemento de ordem finita f.
Então para qq n∈N: $\mathbf{o(a^n) = \frac{f}{mdc(f,n)}}$.

Se não existe nenhum n∈N tq $a^n = 1_G$ então diz-se que a tem ordem infinita e escrevemos **o(a)=∞.**

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∈G. Então, p/ qq inteiro positivo k: $(ab)^k = 1_G \Leftrightarrow (ba)^k = 1_G$.

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

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

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

Teorema de Lagrange: Seje G grupo <u>finito</u> e H<G ⟹ |H| divide por |G|

Teorema de Cauchy: Seje G um grupo de ordem n∈N e p um <u>primo</u> divisor de n. Então, existe um elemento a∈G tq **o(a)=p.**

Sejam G um grupo e ∅ ≠ X ⊆ G.

Chama-se **subgrupo de G gerado por X**, e representa-se por **<X>**, ao menor subgrupo que contém X.

Se X = {a} , então escrevemos **<a>** para representar **<X>** e falamos no **subgrupo de G gerado por a.**

Sejam G e a∈G um elemento com ordem infinita, então <a> tem nº infinito de elementos.

Se $G = < a >$ tem ordem o, então p/ $1 \leq n \leq o - 1$, a^n é gerador de G sse $mdc(n, o) = 1$.

Se por exemplo G=<a> tem ordem vinte, então, a^n é gerador de G sse *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 <u>abeliano</u>, então H<G é **subgrupo normal/invariante** de G (escreve-se $\mathbf{H} \lhd \mathbf{G}$)
Ou seja $\forall\, \mathbf{x} \in \mathbf{G},\ \mathbf{xH} = \mathbf{Hx}$

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

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

Seja G grupo e H $\lhd$ G, então, ao grupo $\mathbf{G/H}$ 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 $\mathbf{T} \lhd \mathbf{G}$. Então $(HT)/_T \cong H/_{(H \cap T)}$.

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

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 $\mathbf{\Psi}\colon \mathbf{Gn} \to \mathbf{Gm}$ diz-se um **morfismo, ou homomorfismo**, se: $\forall \mathbf{x}, \mathbf{y} \in \mathbf{Gn}$, $\mathbf{\Psi}(\mathbf{xy}) = \mathbf{\Psi}(\mathbf{x})\mathbf{\Psi}(\mathbf{y})$

Um morfismo diz-se um **epimorfismo** se for uma aplicação <u>sobrejetiva</u>, isto é se: $\forall \mathbf{y} \exists \mathbf{x}, \mathbf{Y}(\mathbf{x}) = \mathbf{y}$

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

Um morfismo diz-se **isomorfismo** se for uma aplicação <u>bijetiva</u> (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 $\psi\colon Gn \to Gm$ um <u>morfismo</u> de grupos
Chama-se **núcleo** (ou kernel) de ψ, e representa-se por **Nuc** ψ (ou ker ψ), ao subconjunto de Gn:
$\mathbf{Nuc}\,\psi = \{\mathbf{x} \in \boldsymbol{G_n} \mid \boldsymbol{\psi}(\mathbf{x}) = \mathbf{1_{Gm}}\}$

Sejam G um grupo e H⊲G, então:

$$\begin{aligned} pi\colon G &\longrightarrow G/H \\ x &\longmapsto xH \end{aligned}$$

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

Sejam Gn e Gm dois grupos; se **Ψ: Gn ⟶ Gm** é um momorfismo, então: $\mathbf{\Psi(1_{Gn}) = 1_{Gm}}$.

Sejam Gn e Gm dois grupos e **Ψ: Gn ⟶ Gm** um momorfismo, então: $[\mathbf{\Psi}(\mathbf{x})]^{-1} = \mathbf{\Psi}(\mathbf{x^{-1}})$.

Sejam Gn e Gm dois grupos, H⊆Gn e ψ:Gn⟶Gm um morfismo, então: $H < Gn \Rightarrow \psi(H) < Gm$.

Seja ψ:Gn->Gm um morfismo de grupos. Se ψ é um monomorfismo então $Gn \cong \psi(Gn)$.

Sejam Gn e Gm dois grupos, H ⊆ Gn e ψ:Gn⟶Gm um epimorfismo. Então, H⊲Gn ⇒ ψ(H) ⊲Gm.

Seja ψ:Gn⟶Gm um morfismo de grupos. Então, ψ é um monomorfismo se e só se $Nuc\psi = \{1_{Gn}\}$.

Seja ψ:Gn⟶Gm um morfismo de grupos definido por $\psi(x) = 1G_m\ (\forall x \in G_n)$. Então ψ é morfismo de grupos **nulo**.

Teorema Fundamental do Homomorfismo:
Seja θ:G⟶G' um morfismo de grupos. Então, Im θ ≅ G/Nucθ.

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 ·, nele definidas. O triplo **(A,+,·)** diz-se um **anel** se:

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

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

Seja (A,+,·) um anel:
> Ao elemento neutro do grupo chamamos **zero do anel** e representamos por $\mathbf{0_A}$
> Quando existe, ao elemento neutro do semigrupo chamamos **identidade do anel** e representamos por $\mathbf{1_A}$
> No caso de o anel ter identidade, podem existir elementos que admitem elemento oposto p/ multiplicação
> para todo $x \in \mathbf{A}$, $\mathbf{0_A x = x0_A = 0_A}$
> se a+a=a e a·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 $m,n \in Z$, 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∈N e $a, b_1, b_2, \ldots, b_n \in A$. Então:
1) $a(b_1+b_2+\ldots+b_n) = ab_1+ab_2+\ldots+ab_n$
2) $(b_1+b_2+\ldots+b_n)a = b_1a+b_2a+\ldots+b_na$

Seja A um anel com identidade $\mathbf{1_A}$, um elemento a∈A diz-se uma **unidade** se admite inverso em A.
Representa-se por $\mathbf{U_A}$ o conjunto das unidades de um anel com identidade.

Seje A um anel, um elemento a∈A diz-se **simplificável** se, para todos x,y∈A: **xa=ya** ou **ax=ay** ⇒ **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.

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

No anel $(\mathbb{Z}_n,+,\cdot)$, os divisores de zero são os elementos $[x]_n$, onde mdc(x,n)≠1.
Para um anel (A,+,·), $n \in \mathbb{N}$, os elementos $[x]_n$ com 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 $\mathbf{na=0_A}$, $\forall \mathbf{a} \in \mathbf{A} \Rightarrow \mathbf{n=0}$, A diz-se anel de **caraterística 0** e escreve-se **c(A)=0**;
2) se $(\exists x \in \mathbb{Z}\backslash\{0\})(\forall a \in A)\, \boldsymbol{xa = 0_A}$, A diz-se anel de **carateristica *k*** onde * e escreve-se **c(A)=*k***.

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

Sejam $A \neq \{0_A\}$ um anel com identidade 1_A e $n \in \mathbb{N}$. Então, c(A)=n ⇔ $o(1_A)$=n.
Seja A um anel e a um elemento de A: c(A)=k ; o(a)=x ; então $\forall b \in A$ - $\mathbf{kb = 0_A} \Rightarrow \mathbf{x \mid k}$.
Se A tem caraterística finita, então a c(A) é o mmc entre as ordens de todos os seus elementos.
Seje $\mathbb{Z}_n$ um anel, $c(\mathbb{Z}_n)=n$ e $c(\mathbb{Z}_n \times \mathbb{Z}_n)=n$. **Por fim, anéis de caraterísitcas iguais são isomorfos.**

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

$\mathcal{U}_D$ representa o conjunto das unidades de D – i.e., o conjunto dos elementos para os quais existe $u^{-1} \in D$.
Como $1_D \in D$, temos $\mathcal{U}_D \neq \emptyset$. Pela definição de D.I., 0_D é o único divisor de zero.

Seje D um D.I., dados $x, y \in D$ diz-se que x divide y (ou que x é fator de y, ou y é divisível por x) se, $\exists \boldsymbol{t} \in \boldsymbol{D}$: $\boldsymbol{t} = \boldsymbol{y} \,|\, \boldsymbol{x}$.

Um elemento p diz-se **irredutível** em D se:
1) $p \neq 0_D$ e $p \in \mathcal{U}_D$;
2) $p = ab \Longrightarrow a \in \mathcal{U}_D$ ou $b \in \mathcal{U}_D$.

Um elemento p diz-se primo em D se:
1) $p \neq 0_D$ e $p \notin \mathcal{U}_D$;
2) $p | ab \Longrightarrow p | a$ ou $p | a$.

Todo o elemento primo de D é um elemento irredutível.

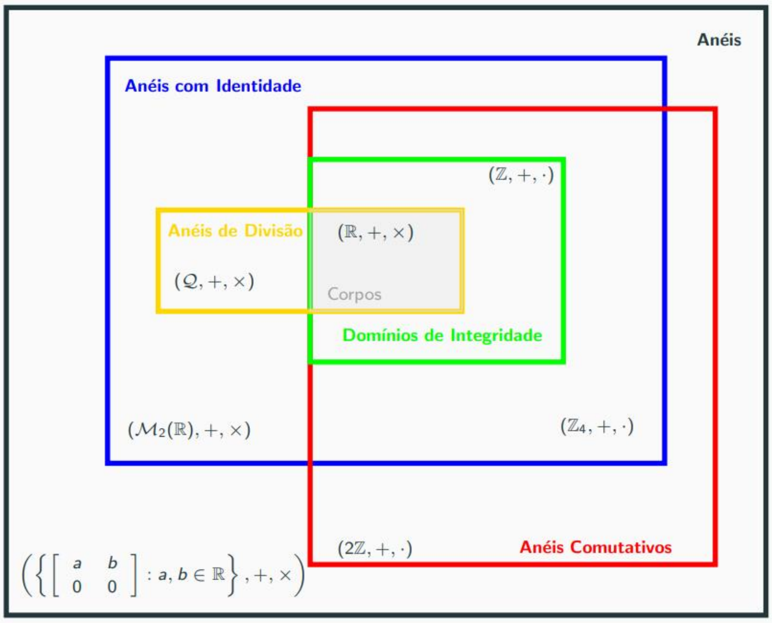
De alguma forma, num corpo todos elementos primos são irredutíveis (e vice-versa), e também não há elementos irredutíveis.

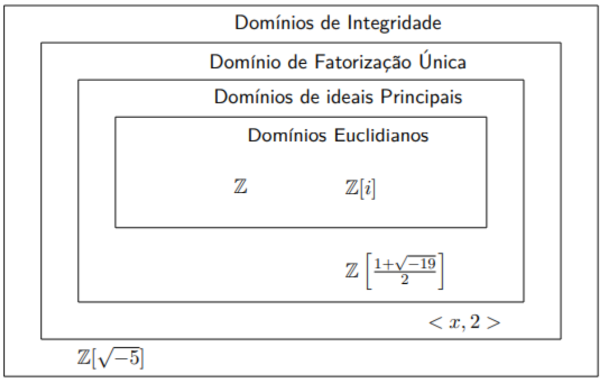
Um anel A diz-se um **anel de divisão** se $(A\backslash\{0_A\}, \cdot)$ é um grupo.
Um anel de divisão comutativo diz-se um **corpo**.
Resulta da definição que qq corpo é um domínio de integridade (o recíproco não é verdadeiro).

Um D.I. diz-se um **domínio euclidiano** se for possível definir uma aplicação $\delta: D \longrightarrow \mathbb{N}_0$ tq:
1) $\forall a, b \in D\backslash\{0_D\}$ $\quad b | a \Longrightarrow \delta(b) \leq \delta(a)$;
2) se $a, b \in D$ e $b \neq 0_D$, então, existem $q, r \in D$ tq $a = bq + r$ e $\delta(r) \leq \delta(b)$.

À aplicação $\boldsymbol{\delta}$ chama-se valoração em D.

Seje D um domínio euclidiano. Então, $\forall b \in D\backslash\{0_D\}$ $\delta(0_D) < \delta(b)$.





Sejam A um anel e A’⊆A. Então, A’ é **subanel** de A sse:
1) A≠ ∅
2) x,y∈A’⟹ x-y∈A’
3) x,y∈A’⟹ xy∈A’

Sejam A um domínio de integridade e A’⊆A.
Então, A’ é **subdomínio** de integridade de A sse:
1) 1_A∈A’
2) x,y∈A’⟹ x-y∈A’
3) x,y∈A’⟹ xy∈A’

Sejam A um anel de divisão (respetivamente, **corpo**) e A’⊆A.
Então, A’ é subanel de divisão (respetivamente, **subcorpo**) de A sse:
1) A’≠∅
2) x,y∈A’⟹ x-y∈A’
3) x,y∈A’\\{0_A}⟹ xy^{-1}∈A’\\{0_A}

Seja A um anel, I é **ideal** de A se:
1) (I, +) < (A, +)
2) ∀x∈A ∀i∈I, xi,ix∈I   (I⊆A, I≠ ∅)

Se apenas xi∈I, então dizia-se ideal esquerdo; caso apenas ix∈I dizia-se ideal direito.

Todo ideal de um anel A é um subanel de A.

Ideial próprio: **I=A se 1_A ∈ I**
- I⊆A mas I≠A

Seja A um anel comutativo com identidade, um ideal I diz-se **ideal maximal** de A se <u>não existe</u> K ideal de A tq: **I ⊈ K ⊈ A.** Se existir K⊆A tq I ⊈ K então I=K.

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

Seje A um anel comutativo com identidade. Um ideal I de A diz-se primo se A\I ≠ ∅ e A\I é fechado p/ o produto.

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

- I é maximal - I é ideal primo
- A/I é corpo - A/I é um domínio de integridade

→ Também isto significa que A/I é um anel comutativo.

Se A é um anel com identidade $\mathbf{1_A}$, então A/I é um anel com identidade $\mathbf{1_A+I}$

I ideal maximal ⇔ A/I corpo ⟹ A/I domínio de integridade ⇔ I ideal primo

Se considerarmos o anel $\mathbb{Z}$, um ideal é maximal sse é do tipo $p\mathbb{Z}$, com p primo, pois $p\mathbb{Z}$ só é corpo se p for primo.

Sejam A e A' dois anéis.
Uma aplicação φ:A→A' diz-se um **morfismo** (ou homomorfismo) de anéis se satisfaz as seguintes condições:

1) (∀a,b∈A) φ(a+b) = φ(a)+φ(b)
2) (∀a,b∈A) φ(a·b) = φ(a)·φ(b)

Um morfismo diz-se: **monomorfismo** se for injetivo; **epimorfismo** se sobrejetivo; **isomorfismo** caso bijetivo.

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

Seja $\varphi: A \longrightarrow A'$ um morfismo de anéis: (ou Ker φ)

1) Chama-se **Núcleo** de φ (ou kernel) – **Nuc φ** – ao subconjunto de A definido por: Nuc φ = $\{x \in A: \varphi(x) = 0_A\}$
2) Chama-se **Imagem** de φ - **Im φ** ou $\boldsymbol{\varphi(A)}$ – ao subconunto de A' definido por: Im φ = $\{\varphi(x): x \in A\}$

Também: Nuc φ é um ideal de A; Im φ é subanel de A'.

Sejam A e A' dois anéis e φ:A⟶A' um morfismo.
Então: $\varphi(0_A)=0_{A}$; (∀a∈A) φ(-a) = $-\varphi$(a) ; (∀a∈A) (∀k∈Z) φ(ka) = kφ(a)
Também se A' é comutativo e φ é monomorfismo, então A é comutativo.

Sejam φ:A⟶A' um morfismo de anéis e B um subanel de A. Então, φ(B) é um subanel de A'.

Sejam φ:A⟶A' um epimorfismo de anéis e I um ideal de A. Então, φ(I) é um ideal de A'.

Seja φ:A⟶A' um morfismo não nulo de anéis, se A é um corpo, então, φ(A) é um corpo.

Seja φ:A⟶A' um morfismo de anéis, então $A/Nuc\,\varphi$ é isomorfismo a φ(A)

Seja A um anel e I um seu ideal. Então a aplicação $\pi: A \longrightarrow A/I$ definida por $\pi(x) = x + I (x \in A)$ é um epimorfismo (ao qual se chama <u>epimorfismo canónico</u>).

Seje $f: \mathbb{Z} \longrightarrow \mathbb{Z}_{10}$ um morfismo de anéis definido por $f(x) = [kx]_{10}$ $(\forall x \in \mathbb{Z})$.

$$\forall x, y \in \mathbb{Z},\ f(xy) = f(x)f(y) \Leftrightarrow [kxy]_{10} = [k^2xy]_{10} \Leftrightarrow k \equiv k^2 (\text{mod } 10) \Leftrightarrow k \in \{1{,}5\}$$

O único morfismo de anéis de uma aplicação $f: \mathbb{R} \longrightarrow \mathbb{Z}$ ou $f: \mathbb{Q} \longrightarrow \mathbb{Z}$ (entre $\mathbb{R}$ e $\mathbb{Z}$ ou $\mathbb{Q}$ e $\mathbb{Z}$), é o morfismo nulo.

Teorema Fundamental do Homomorfismo: Seja $\varphi: A \longrightarrow A'$ um morfismo de anéis, então existe um ideal I de A tq: $\boldsymbol{A/I \cong \varphi(A)}$

1º Teorema do Isomorfismo: Seja $\varphi: A \longrightarrow A'$ um epimorfismo de anéis. Se I é ideal de A tq $Nuc\,\varphi \subseteq I$, então: $\boldsymbol{A/I \cong A'/\varphi(I)}$

2º Teorema do Isomorfismo: Sejam A um anel e A_1 e A_2 seus subanéis. Se A_2 é um ideal de A, então:

$$(\boldsymbol{A_1} + \boldsymbol{A_2})/\boldsymbol{A_2} \cong \boldsymbol{A_1}/(\boldsymbol{A_1} \cap \boldsymbol{A_2})$$

Permutações

Seje 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

$$|<\sigma>| = o(\sigma) = x$$