**Nota**

p/ - para

qq - qualquer

tq - tal que

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)

**a ≡ b (mod n) -> a − b = kn**

Uma função diz-se **injetiva** se p/ cada elemento , existe um único tq .

Uma função diz-se **sobrejetiva** se p/ cada elemento , existe pelo menos um tq .

Uma função 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 um grupóide.

Um elemento diz-se um **elemento zero/nulo** se .

Um elemento diz-se um **elemento neutro/identidade** se .

Um elemento diz-se um **elemento idempotente** se . Um elemento neutro/nulo é um elemento idempotente.

Num grupóide existe no máximo um elemento neutro – representado por .

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

Seja S um semigrupo, e , então:

1. [];
2. [].

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

Seja um monóide.

Um elemento diz-se um elemento oposto de se .

Um elemento , tem no máxmio, um elemento oposto.

**Oposto:**

inverso de a = [Linguagem Multiplicativa]

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

simétrico de a = -a [Linguagem Aditiva]

**--------------------**

**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)**

(se qualquer elemento de G admita um elemento identidade que pertença a G)

**3)**

(se para qualquer elemento de G haja um elemento oposto pertencente a G)

Seje G um grupo:

> =

> ()•() =

> =

> =

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

> = ()•()

> = ()...()

> são válidas as **leis de corte**: para

Também a igualdade 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

**\***se G é grupo e S<G então o elemento neutro de S é o mesmo que o de G . Pois por um lado temos que, ; por outro lado, como ∈G, temos que . Logo pela lei do corte,

- x∈S ∈S

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 então

**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 - representa-se por – dito de outra forma, se: a) ; b)

Seja G grupo e aG um elemento de ordem finita f.

Então para qq n∈N: **o()= .**

Se não existe nenhum n∈N tq 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: .

Sejam G um grupo e a∈G, então: **o()= o().**

Se então ).

**Teorema de Lagrange:** Seje G grupo finito e H<G |H| divide por |G|

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

Sejam G um grupo e .

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 tem ordem *o*, então p/ , é gerador de G sse .

Se por exemplo G=<a> tem ordem vinte, então, é gerador de G sse *mdc(n,20)=1*, ou seja, sse . Logo G tem 8 geradores.

Seja G um grupo abeliano, então H<G é **subgrupo** **normal/invariante** de G (escreve-se )

Ou seja **,**

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

Seja G grupo e H<G e H’G. Então, HH’G. Também se H’H, então H’H.

Seja G grupo e HG, então, ao grupo chama-se **grupo quociente** (que é abeliano)

**Demonstração:** Sejam , então,

**2º Teorema do Isomorfismo –** Sejam G grupo e tq . Então .

**Grupo Cíclico:**  , i.e, se existe tq –

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, GZp (G é isomorfo a Zp).

Uma aplicação diz-se um **morfismo**, **ou homomorfismo**, se:

Um morfismo diz-se um **epimorfismo** se for uma aplicação sobrejetiva, isto é se:

Um morfismo diz-se um **monomorfismo** se for uma aplicação injetiva, isto é sse:

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 um morfismo de grupos

Chama-se **núcleo** (ou kernel) de , e representa-se por **Nuc**  (ou ker ), ao subconjunto de Gn:

Sejam G um grupo e HG, então:

pi: G ⟶ G/H

x ⟼ xH

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: **Ψ()=.**

Sejam Gn e Gm dois grupos e **Ψ: Gn ⟶ Gm**  um momorfismo, então: **.**

Sejam Gn e Gm dois grupos, H⊆Gn e ψ:Gn⟶Gm um morfismo, então: .

Seja ψ:Gn->Gm um morfismo de grupos. Se ψ é um monomorfismo então Gnψ(Gn).

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

Seja ψ:Gn⟶Gm um morfismo de grupos. Então, ψ é um monomorfismo se e só se .

Seja ψ:Gn⟶Gm um morfismo de grupos definido por . Então ψ é morfismo de grupos **nulo**.

**Teorema Fundamental do Homomorfismo:**

Seja θ:G⟶G′ um morfismo de grupos. Então, Im θG/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

**>** Quando existe, ao elemento neutro do semigrupo chamamos **identidade do anel** e representamos por

**>** No caso de o anel ter identidade, podem existir elementos que admitem elemento oposto p/ multiplicação

**>** para todo x**A,**

**>** se a+a=a e a∙a=a, é um anel comutativo com identidade, chamamos A um **anel nulo**

**>** sejam x,yA, então, e

Sejam a,bA e m,nZ, então:

- (m+n)a = ma+na

- n(ma) = (nm)a

- n(a+b) = na+nb

- n(ab) = (na)b = a(nb)

-

-

**Propriedade Distributiva Generalizada**

Sejam A um anel, n∈N e a,,, ...,∈A. Então:

1) a(++...+) = ++...+

2) (++...+)a = ++...+

Seja A um anel com identidade , um elemento a∈A diz-se uma **unidade** se admite inverso em A.

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

Para um anel (A,+,∙), n∈N, os elementos com mdc(x,n)=1 são as unidades do anel.

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

Num anel A, toda a unidade é simplificável, mas nem todo o elemento simplificável é uma unidade

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

No anel (,+,∙), os divisores de zero são os elementos , onde mdc(x,n)1

Seja A um anel:

1. se **na=**, , A diz-se anel de **caraterística** **0** e escreve-se **c(A)=0**;
2. se , A diz-se anel de **carateristica** ***k*** onde \* e escreve-se **c(A)=*k***

\*

Sejam A{} um anel com identidade e n∈N. Então, c(A)=no()=n.

**Domínio de Integridade –** um anel comutativo com identidade tq é o único divisor de zero

Se A é um domínio de integridade, então, A{}

O anel A é um domínio de integridade

Então, seja A um anel comutativo as próximas afirmações são equivalentes com a afirmação acima:

- A\{} e todo o elemento de A\{} é simplificável

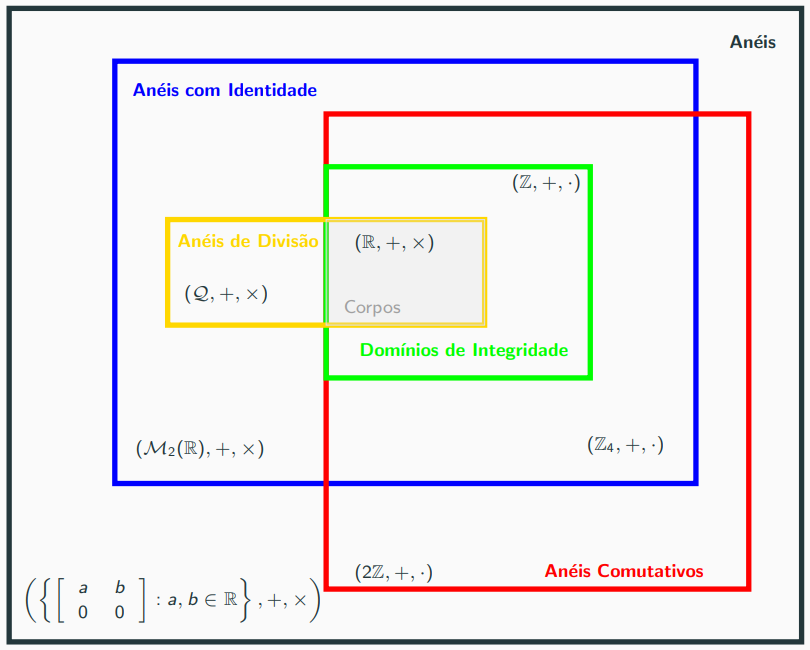
- A\{} e A\{} é subsemigrupo de A relativamente ao produto

- A\{} e, se as equações *ax=b* e *xa=b (a)* tiverem solução, então, a solução é única

Um anel A diz-se um **anel de divisão** se (A\{},∙) 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′⊆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) ∈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′\{}x∈A′\{}

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

1. (I, +) < (A, +)
2. ∀x∈A ∀i∈I, xi,ix∈I (IA, I)

Todo ideal de um anel A é um subanel de A

**Ideial próprio:**

- IA

- IA mas IA

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

Se existir KA tq IK então I=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 se I**

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 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 ϕ:A->A′ um morfismo. Então, ϕ()=

Sejam A e A′ dois anéis e ϕ:A->A′ um morfismo. Então, (∀a∈A) ϕ(−a) = −ϕ(a)

Sejam A e A′ dois anéis e ϕ:A->A′ um morfismo. Então, (∀a∈A) (∀k∈Z) ϕ(ka) = kϕ(a)

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 é isomorfismo a ϕ(A)

**-------------------**

**Permutações**

**-------------------**

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

Se A é um conjunto de , 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

**|<σ>| = o(σ)=x**

