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 $x \in X$, 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•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.

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:

> $id^{-1} = id$
> $(x^m)\bullet(x^n) = x^{m+n}$
> $(x^m)^n = x^{m\bullet n}$
> $(a^{-1})^{-1} = a$
> $(a \bullet b)^{-1} = (b^{-1})\bullet(a^{-1})$
> $(a_1 \ldots a_n)^{-1} = (a_n{}^{-1})\ldots(a_1{}^{-1})$
> 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).

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 $\boldsymbol{o}([\boldsymbol{a}]_{\boldsymbol{p}})$ - também, para $\boldsymbol{o(a) = k}$, se: $a^k = 1_G$; $p \in \mathbb{N}$, $a^p = 1_G \Rightarrow k \leq p$

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

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: $\mathbf{o}(\boldsymbol{a^{-1}}) = \mathbf{o}(\boldsymbol{a})$.

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

Seja G um grupo <u>abeliano</u>, então H<G é **subgrupo normal/invariante** de G (escreve-se H⊲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, então, ao grupo $\mathbf{G/H}$ chama-se **grupo quociente** (que é abeliano)

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

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

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 n, então, $G \cong Zn$.

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

Uma aplicação $\mathbf{\Psi}\colon \mathbf{Zn} -> \mathbf{Zm}$ diz-se um **morfismo, ou homomorfismo**, se: $\forall \mathbf{x}, \mathbf{y} \in \mathbf{Gn}\ \ \mathbf{\Psi(xy)} = \mathbf{\Psi(x)\Psi(y)}$

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

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

Um morfismo diz-se **isomorfismo** se for uma aplicação <u>bijetiva</u> (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 $\psi\colon Gn -> Gm$ 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:
$\mathbf{Nuc}\,\psi = \{\mathbf{x} \in \mathbf{Gn} \mid \boldsymbol{\psi}(\mathbf{x}) = \mathbf{1_{Gm}}\}$

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: $[\mathbf{\Psi(x)}]^{-1} = \mathbf{\Psi(x^{-1})}$.

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 $Nuc\psi = \{1_{Gn}\}$.

Teorema Fundamental do Homomorfismo:
Seja θ:G->G′ um morfismo de grupos. Então, $Im\ \theta \cong G/Nuc\theta$.

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 ·, 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 <u>se a multiplicação for comutativa</u>.

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 para a multiplicação
> para todo x ∈ **A**, $\mathbf{0_A x = x 0_A = 0_A}$
> se a+a=a e a·a=a, é um anel comutativo com identidade, chamamos A um **anel nulo**
> sejam x,y ∈ A, então, $(-x)y = x(-y) = -xy$ e $(-x)(-y) = xy$

Sejam a,b ∈ A e m,n ∈ 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, ..., b_n∈A. Então:
1) $a(b_1 + b_2 + ... + b_n) = ab_1 + ab_2 + ... + ab_n$
2) $(b_1 + b_2 + ... + b_n)a = b_1 a + b_2 a + ... + b_n a$

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.

Para um anel (A,+,·), n∈N, os elementos $[x]_n$ 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=ay** ⇒ **x=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\{0_A} tq: **ab=$\mathbf{0_A}$** ou **ba=$\mathbf{0_A}$**

No anel (Z_n,+,·), os divisores de zero são os elementos $[x]_n$, onde mdc(x,n)≠1

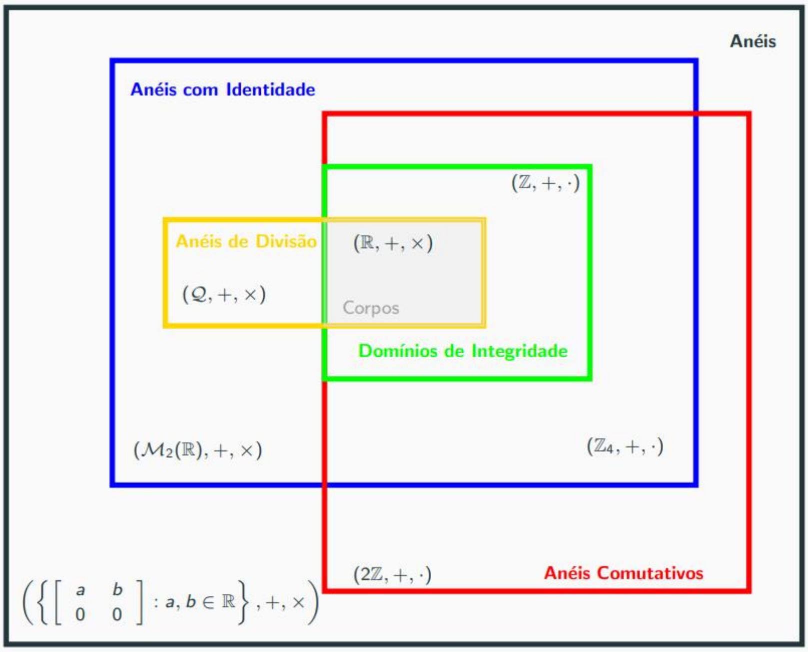
Seja A um anel:
1) se não existir qq n∈N tq **na=$\mathbf{0_A}$** , ∀a∈A, A diz-se anel de **caraterística** 0 e escreve-se **c(A)=0**
2) se n∈N for o menor natural tq **na=$\mathbf{0_A}$**, ∀a∈A, **c(A)=n**

Sejam A≠{0_A} um anel com identidade 1_A e n∈N. Então, a c(A)=n ⟺ o(1_A)= n.
Domínio de Integridade – um anel comutativo tq 0_A é o único divisor de zero

Se A é um domínio de integridade, então, A≠{0_A}

O anel A é um domínio de integridade
Então, seja A um anel comutativo as próximas afirmações são <u>equivalentes com a afirmação acima:</u>
- A\{0_A}≠ ∅ e todo o elemento de A\{0_A} é simplificável
- A\{0_A}≠ ∅ e A\{0_A} é subsemigrupo de A relativamente ao produto
- A\{0_A}≠ ∅ e, se as equações *ax=b* e *xa=b* *(a≠ 0_A)* tiverem solução, então, a solução é única

Um anel A diz-se um **anel de divisão** se (A\{0_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) 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≠ ∅)

Todo ideal de um anel A é um subanel de A

Ideial próprio:
- I⊈A
- 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

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 $1_A \in I$

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, $\varphi(0_A) = 0_A$

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 $A/Nuc\,\varphi$ é isomorfismo a φ(A)

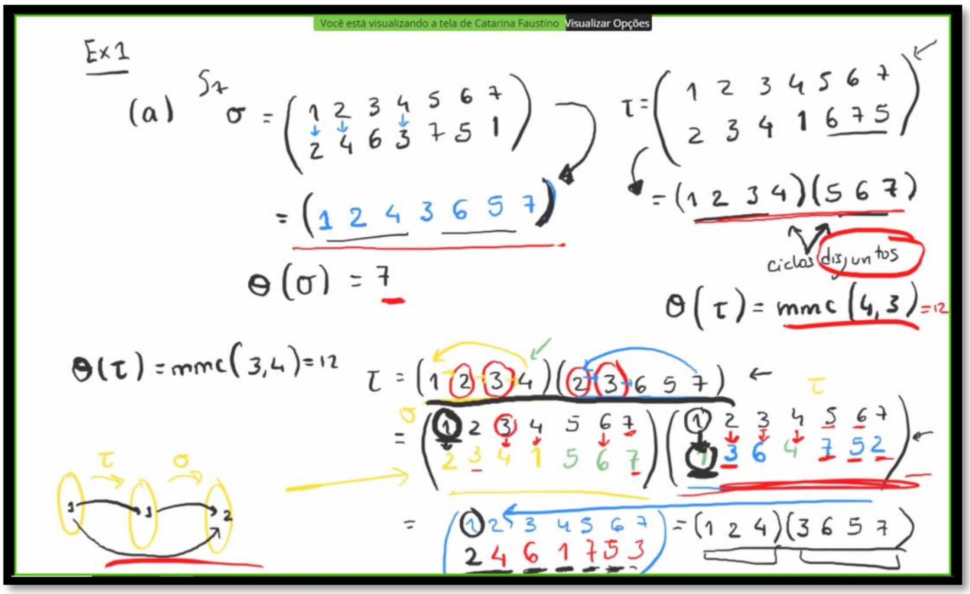
Permutações

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

Se A é um conjunto de $n \in \mathbb{N}$, 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

|<σ>| = o(σ)=x



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

Por uma Proposição

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

A 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 $\underline{n}$ tq

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

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

I ideal de A $\boxed{(I \subseteq A, I \neq \emptyset)}$ F

(0)

(i) $(I, +) < (A, +)$ ←

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

$\varphi(I)$

(c) $a, b \in A$

$$(a+b)(a-b) = a \cdot a + a \cdot (-b) + b \cdot a + b \cdot (-b)$$
$$= a^2 - ab + ba - b^2$$

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 existir $b \in A \setminus \{0_A\}$ tal que

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

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

(h) Sejam I, J ideais próprios de A.

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

$$? \; I = J \; ?$$

É claro que

$$I \cap J \subsetneq I \quad (1)$$
$$I \cap J \subseteq J \quad (2)$$

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

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

logo $I = I \cap J = J$ ✓

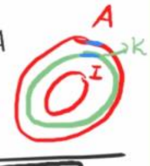
I ideal próprio: $I \subsetneq A$

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

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

$$I \subsetneq K \subsetneq A$$

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



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

$1_A \; (A, \cdot)$