$$\mathbb{Z}/(p) \begin{cases} (\mathbb{Z}, +) \text{ Abelian Group} \\ (p) = \text{Multiples of the number } p \in \mathbb{Z} \longrightarrow \text{Subgroup of } (\mathbb{Z}, +) \end{cases}$$

Example: $\mathbb{Z}/(4)$

cryptography

$$\bar{0} = \underbrace{\{\ldots, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\}}_{(4)}$$

$$\bar{1} = 1 + (4) = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$$

$$\bar{2} = 2 + (4) = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$$

$$\bar{3} = 3 + (4) = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$$

$$\bar{4} = 4 + (4) = \{\ldots, -4, 0, 4, 8, 12, \ldots\} = \bar{0}$$

$$\mathbb{Z}/(4) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$$

$$\bar{a} + \bar{b} = \overline{a+b}$$

$$(\mathbb{Z}_4, +)$$

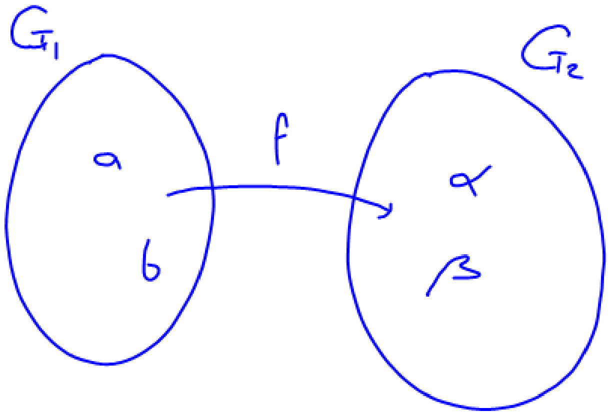
	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$$\bar{2} + \bar{3} = \overline{2+3} =$$
$$= \bar{5} = \bar{1}$$

$$\overline{36} = \bar{0} \qquad 36 \,\underline{|\, 4} \quad (0) \;\; 9$$

$$\overline{37} = \bar{1} \qquad 37 \,\underline{|\, 4} \quad (1) \;\; 9$$

Homomorphisms   Linear Aplications



$$(G_1, *) \xrightarrow{f} (G_2, \Delta)$$

$\forall a, b \in G_1$ $\qquad$ $\forall \alpha, \beta \in G_2$

$a * b \in G_1$ $\qquad$ $\alpha \,\Delta\, \beta \in G_2$

$e_1 \equiv$ Neutral of G_1 $\qquad$ $e_2 \equiv$ Neutral of G_2

If $f(a) = \alpha \ \wedge\ f(b) = \beta$

$$\boxed{f \text{ will be a homomorphism} \iff \begin{cases} f(a * b) = f(a) \,\Delta\, f(b) \\ \wedge \longrightarrow \text{AND} \\ f(e_1) = e_2 \end{cases}}$$

IF AND ONLY IF

$f : G_1 \longrightarrow G_2$

Homomorphism

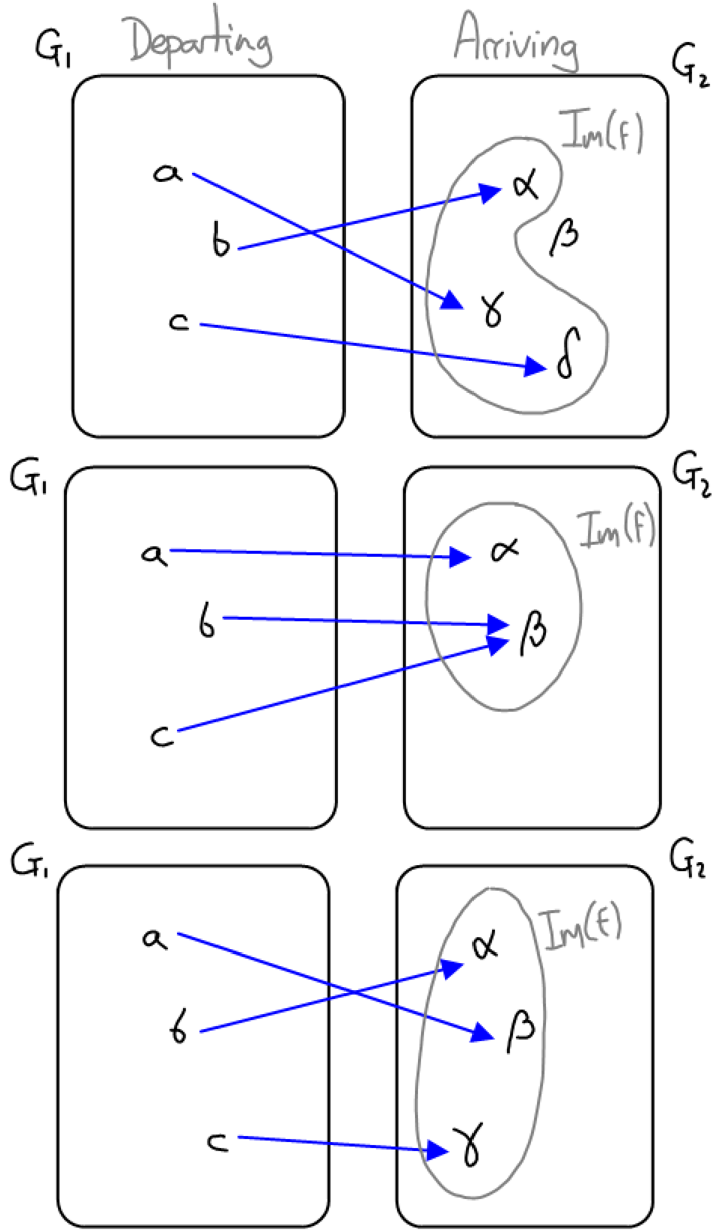
Inyectivity ≡ Every element has an Image and that image is unique

$$\begin{cases} \text{If } f(a)=f(b) \longrightarrow a=b & \forall a,b \in G_1 \\ \text{If } a \neq b \longrightarrow f(a) \neq f(b) & \forall a,b \in G_1 \end{cases}$$

Suprayectivity ≡ Every element from the arriving group belongs to Im(f), but it doesn't need to be unique.

$$\forall y \in G_2 \quad \exists x \in G_1 \ / \ f(x)=y$$

Biyectivity ≡ Inyective + Suprayective



$$\boxed{f : G_1 \longrightarrow G_2}$$

f	$G_1 \neq G_2$	$G_1 = G_2$
Not Biyective	Homomorphism	Endomorphism
Biyective	Isomorphism	Automorphism

Rings $(R, *, \Delta)$ ILC's

R is a Ring $\Longleftrightarrow$

- $(R, *)$ is an Abelian Group
  - Internal $\forall a,b \in R \quad a*b \in R$
  - Asociative $\forall a,b,c \in R \quad a*(b*c) = (a*b)*c$
  - Neutral $\exists! e \in R \quad e*a = a*e = a \quad \forall a \in R$ → The 0 of the ring
  - Symmetrical $\forall a \in R \ \exists a' \in R \quad a*a' = a'*a = e$
  - Abelian: $\forall a,b \in R \quad a*b = b*a$
- (R, Δ) is a semigroup
  - Internal $\forall a,b \in R \quad a \Delta b \in R$
  - Asociative $\forall a,b,c \in R \quad a\Delta(b\Delta c) = (a\Delta b)\Delta c$
- Distributives: $a*(b\Delta c) = (a*b)\Delta(a*c) \ \wedge \ a\Delta(b*c) = (a\Delta b)*(a\Delta c)$

An Abelian Ring ⟶ $\forall a,b \in R \quad a\Delta b = b\Delta a$

A Unitary (or Unity) Ring ⟶ $\exists! 1_R \in R$ ⟶ $a\Delta 1_R = 1_R \Delta a = a$ 1_A → The 1 of the ring

We will say a Ring is Nondivisible by 0 ⟶ $\forall a,b \in R \quad a\Delta b \neq 0_R$

We will say a Ring is Divisible by 0 ⟶ $\exists a,b \in R \quad a\Delta b = 0_R$

Example of divisors of 0:

$(\mathbb{Z}/_{(6)}, +, \cdot)$ UNITARY ABELIAN RING

$\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

$\bar{a} + \bar{b} = \overline{a+b}$

$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$

$\boxed{\bar{2} \cdot \bar{3} = \bar{0}}$

Body $(B, *, \Delta)$

B is a BODY $\iff$ B is a UNITARY, ABELIAN, NONDIVISIBLE by 0 Ring

The multiplicative group of B is $\boxed{(B - \{0_B\}, \Delta) \text{ Abelian Group}}$

Neutral element with $*$

Vector Space

$V(B)$ is a vector space $\Longleftrightarrow$

- V is an ABELIAN GROUP whose elements $\forall \bar{v} \in V$ are called vectors
- B is a BODY whose elements $\forall \lambda \in B$ are callad scalars
- There is an ELC between V and B $\forall \lambda \in B \wedge \forall \bar{v} \in V \rightarrow \lambda \cdot \bar{v} \in V$
- There is a DOUBLE DISTRIBUTIVE $\forall \lambda, \mu \in B\ \forall \bar{u}, \bar{v} \in V$ $\begin{cases} \lambda \cdot (\bar{u} + \bar{v}) = \lambda \cdot \bar{u} + \lambda \cdot \bar{v} \\ (\lambda + \mu) \cdot \bar{u} = \lambda \bar{u} + \mu \cdot \bar{u} \end{cases}$
- There is an External Asociative: $(\lambda \cdot \mu) \cdot \bar{u} = \lambda \cdot (\mu \cdot \bar{u})$

External Law of Composition

$$\text{ILC} \begin{cases} (V, +) & \bar{u} + \bar{v} \in V \\ (B, + \cdot) & \lambda + \mu \in B \\ & \lambda \cdot \mu \in B \end{cases}$$

$$\text{ELC} \left\{ \cdot : B \times V \longrightarrow V \qquad \lambda \cdot \bar{u} \in V \right.$$

Vector subspace Given $V(\mathbb{R})$ a vector space and $S \subseteq V$

$\hookrightarrow (\mathbb{R}, +, \cdot)$ Body

$S(\mathbb{R})$ is a subspace of $V(\mathbb{R}) \Longleftrightarrow \boxed{\forall \lambda, \mu \in \mathbb{R}} \wedge \boxed{\forall \bar{u}, \bar{v} \in S} \rightarrow \boxed{\lambda \bar{u} + \mu \bar{v} \in S}$

Example: Given $\mathbb{M}_2(\mathbb{R})$ Vector space of order 2 regular matrixes

Prove that $\mathbb{S}_2(\mathbb{R})$ is a subspace of $\mathbb{M}_2$ (where $\mathbb{S}_2$ is the set of symmetrical matrixes in $\mathbb{M}_2$)

$\hookrightarrow S = S^t$ when S is symmet.

$$\mathbb{M}_2(\mathbb{R}) = \left\{ M \in \mathbb{M}_2 \;/\; M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \forall a, b, c, d \in \mathbb{R} \right\}$$

$$\mathbb{S}_2(\mathbb{R}) = \left\{ S \in \mathbb{S}_2 \;/\; S = \begin{pmatrix} \alpha & \gamma \\ \gamma & \beta \end{pmatrix} \forall \alpha, \beta, \gamma \in \mathbb{R} \right\}$$

$\boxed{\forall \lambda, \mu \in \mathbb{R}}$

$\boxed{\forall S_1 = \begin{pmatrix} a & c \\ c & b \end{pmatrix}, S_2 = \begin{pmatrix} d & f \\ f & e \end{pmatrix} \in \mathbb{S}_2}$

$$\lambda S_1 + \mu S_2 = \lambda \begin{pmatrix} a & c \\ c & b \end{pmatrix} + \mu \begin{pmatrix} d & f \\ f & e \end{pmatrix} = \begin{pmatrix} \lambda a & \lambda c \\ \lambda c & \lambda b \end{pmatrix} + \begin{pmatrix} \mu d & \mu f \\ \mu f & \mu e \end{pmatrix} =$$

$$= \boxed{\begin{pmatrix} \lambda a + \mu d & \lambda c + \mu f \\ \lambda c + \mu f & \lambda b + \mu e \end{pmatrix} \in \mathbb{S}_2}$$

$\mathbb{S}_2$ is a subspace of $\mathbb{M}_2$

<u>Linear composition</u> $\{\bar{u}_i\}$ is a set of vectors of a certain space $V(\mathbb{R})$

We say we have a linear composition of $\{\bar{u}_i\}$, $\mathcal{L}\{\bar{u}_i\}$, when:

$$\mathcal{L}\{\bar{u}_i\} = \lambda_1\bar{u}_1 + \lambda_2\bar{u}_2 + \ldots + \lambda_n\bar{u}_n \quad \forall \lambda_i \in \mathbb{R}$$

<u>Linear dependance</u> We can say that the vector in $\{\bar{u}_i\}$ are linearly DEPENDANT when:

$$\mathcal{L}\{\bar{u}_i\} = \bar{0} \text{ and at least one of the } \lambda_i \text{ is } \underbrace{\lambda_K}_{\text{one of the } \lambda_i} \neq 0$$

<u>Linear independance</u> We can say that the vector in $\{\bar{u}_i\}$ are linearly INDEPENDANT when:

$$\mathcal{L}\{\bar{u}_i\} = \bar{0} \text{ when } \forall \lambda_i = 0$$

Example:

$\{\bar{u}_i\} = \{\underbrace{(1,1,1)}_{\bar{u}_1}, \underbrace{(1,1,0)}_{\bar{u}_2}, \underbrace{(0,0,1)}_{\bar{u}_3}\}$

$\mathcal{L}\{\bar{u}_i\} = \bar{0} \longrightarrow \lambda_1(1,1,1) + \lambda_2(1,1,0) + \lambda_3(0,0,1) = (0,0,0)$

$(\lambda_1+\lambda_2, \lambda_1+\lambda_2, \lambda_1+\lambda_3) = (0,0,0) \longrightarrow \begin{cases} \lambda_1+\lambda_2 = 0 \rightarrow \lambda_2 = -\lambda_1 \\ \cancel{\lambda_1+\lambda_2=0} \\ \lambda_1+\lambda_3 = 0 \rightarrow \lambda_3 = -\lambda_1 \end{cases}$

so for example: if $\lambda_1 = 1 \rightarrow \begin{cases} \lambda_2 = -1 \\ \lambda_3 = -1 \end{cases}$

So I have $\lambda_1 \neq 0$, $\lambda_2 \neq 0$, $\lambda_3 \neq 0$ that make $\mathcal{L}\{\bar{u}_i\} = \bar{0}$

$\{\bar{u}_i\}$ is Linearly Dependant

$\{\bar{v}_i\} = \{\underbrace{(1,1,1)}_{\bar{v}_1}, \underbrace{(1,1,0)}_{\bar{v}_2}, \underbrace{(1,0,0)}_{\bar{v}_3}\}$

$\mathcal{L}\{\bar{v}_i\} = \bar{0} \rightarrow \mu_1(1,1,1) + \mu_2(1,1,0) + \mu_3(1,0,0) = (0,0,0)$

$(\mu_1+\mu_2+\mu_3, \mu_1+\mu_2, \mu_1) = (0,0,0) \longrightarrow \begin{cases} \mu_1+\mu_2+\mu_3 = 0 \longrightarrow \mu_3 = 0 \\ \mu_1+\mu_2 = 0 \longrightarrow \mu_2 = 0 \\ \mu_1 = 0 \end{cases}$

$\mu_1 = \mu_2 = \mu_3 = 0$

$\{\bar{v}_i\}$ is Linearly Independant