f funzione $\quad f \subseteq A \times B$

$f: A \to B \qquad \forall a \in A \; \exists! b \in B : (a,b) \in f$

$f(a) = b$

$f^{-1} : B \to A$ tale che $f^{-1} \circ f : A \to B = id_A$

$f \circ f^{-1} : B \to A = id_B$

esiste $\Leftrightarrow$ f è biiettiva.

$f^{-1} = f^{opp} = \{ (b,a) \in B \times A \mid (a,b) \in A \times B \}$.

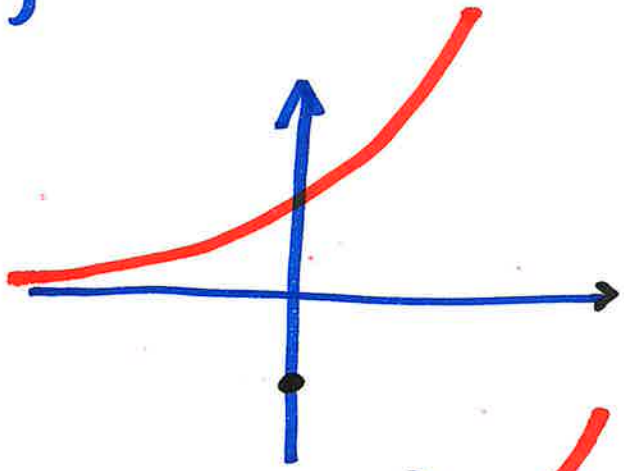
e f^{opp} è funzione $\Leftrightarrow \forall b \in B \; \exists! a \in A : (a,b) \in f$

Se $X \subseteq A$ ed $Im(f_{|X}) \subseteq Y \subseteq B$

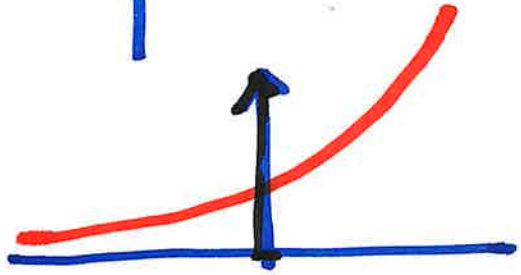
$$f|_X^Y : X \to Y$$

restrizione di f a X tronca a Y

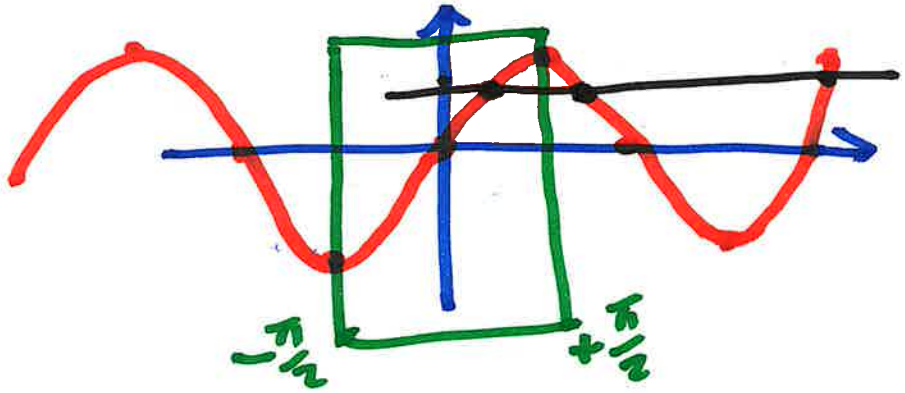
$$\exp : \begin{cases} \mathbb{R} \to \mathbb{R}^* \\ x \to e^x \end{cases}$$



$$\exp|^{]0,+\infty[} : \mathbb{R} \to]0,+\infty[$$



$$\begin{cases} \mathbb{R} \to \mathbb{R} \\ x \to \sin(x) \end{cases}$$



$\sin^{-1}$

$$\sin' : \begin{cases} [-\frac{\pi}{2}, \frac{\pi}{2}] \to \mathbb{R} \\ x \to \sin(x) \end{cases}$$

è iniettiva.

$\sin|_{[-\frac{\pi}{2}, \frac{\pi}{2}]}$

$$\sin'' = \sin|^{[-1,1]}_{[-\frac{\pi}{2}, \frac{\pi}{2}]} : [-\tfrac{\pi}{2}, \tfrac{\pi}{2}] \to [-1,1]$$

è biiettiva.

$$\arcsin := (\sin'')^{-1}$$

$\forall x \in B$ ci si chiede cosa è l'insieme

$$"f^{-1}(x)" := \{ a \in A \mid f(a) = x \}.$$

↖ NON È UNA FUNZIONE $B \to A$

È UNA FUNZIONE

$$B \to 2^A$$

ove $2^A := \{X : X \subseteq A\}$.

PREIMMAGINI DI x

$\lceil$ $f(x) = b$ $\quad x \in A$, $b \in B$ $\rfloor$

$f: A \to B$ funzione

- $b \notin Im(f) \Rightarrow f^{-1}(b) = \emptyset$ l'eq. non ha soluzione in A
- $\exists! a \in A: f(a) = b$ esiste una ed una sola soluzione!

- $\exists$ molti $a \in A$ tali che $f(a)=b$

$$f: \begin{cases} \mathbb{R} \to \mathbb{R} \\ x \to 0 \end{cases}$$

$f(x)=0$

$f^{-1}(0)=\mathbb{R}$

indeterminate

$$g: \begin{cases} \mathbb{R}^2 \to \mathbb{R} \\ (x,y) \to x+y \end{cases}$$

~~$g(x)=0$~~

$g(x,y)=0$

$\{(x,-x) \in \mathbb{R}^2 \mid x \in \mathbb{R}\}$.

$\mathbb{N}$ → insieme dei numeri naturali $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$
0, 1, 2 ...

$\mathbb{Z}$ → insieme dei numeri interi ... -2, -1, 0, 1, ...

$\mathbb{Q}$ → insieme dei numeri razionali $\frac{a}{b}$ $a, b \in \mathbb{Z}, b \neq 0$

$\mathbb{R}$ → insieme dei numeri reali

$\mathbb{C}$ → insieme dei numeri complessi
$\{a + ib \mid a, b \in \mathbb{R}\}$.

Struttura algebrica

→ sia X un insieme; una <u>operazione binaria</u> su X è una funzione $*: X \times X \to X$

Esempio $+: \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ $\quad +(a,b) := a+b$

$(a,b)+$

$(a+b)\cdot c =$ $\quad a\ b + c\ \cdot$

$(a+b)\ c\ \cdot \to (a+b)\cdot c$

$a + b \cdot c$ $\quad a\ b\ c\ \cdot\ + \to (a + bc)$

bc

$*: X \times X \to X$ deve essere una funzione!

$- : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ non è una operazione.

$2 - 3 \notin \mathbb{N}_0$

$\dot{-} : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$

$(x, y) \to \max(x - y, 0)$

Struttura algebrica: $(X, *, \ldots)$

Insieme X + una o più operazioni binarie definite da

$X \times X \to X$

Modello cui vogliamo arrivare è

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

→ **CAMPO** $(\mathbb{K}, +, \cdot)$

$\mathbb{K} = \mathbb{Q}$ $\mathbb{K} = \mathbb{C}$

$\mathbb{K} = \mathbb{F}_q$

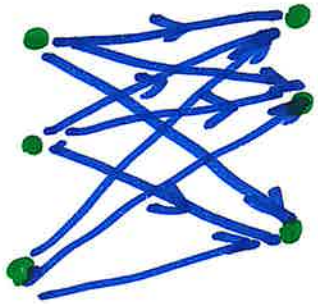
$\mathbb{K} = \mathbb{F}_2 = \mathbb{Z}_2$

$\mathbb{K} = \mathbb{R}(t) =$

$= \left\{ \frac{f(t)}{g(t)} \mid f, g \in \mathbb{R}[t], g \neq 0 \right\}$

↑ polinomi

$$X \times Y = \{(x,y) \mid x \in X,\ y \in Y\}.$$



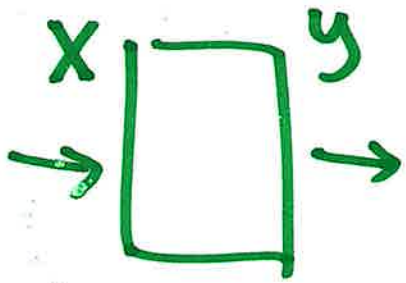
$$(X \times Y)^{app} = Y \times X \qquad X \times X$$

$$R_0 \subseteq X \times Y$$

$$f \subseteq X \times Y \qquad \text{funzione}$$

$$(x,y) \in f \qquad f(x) = y$$

$X \times X \to X$



$f|_X^{|y}$

prima restringere
poi troncare.

$$*: X \times X \to X$$

OPERAZIONE BINARIA SU X $(X, *)$

$(\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}, \cdot)$ è una struttura algebrica

SI DICE CHE $*$ É

- COMMUTATIVA SE
$$\forall x, y \in X : x * y = y * x$$
- AMMETTE EL. NEUTRO SE
$$\exists e \in X : \forall x \in X \quad x * e = e * x = x$$

- AMMETTE INVERSI

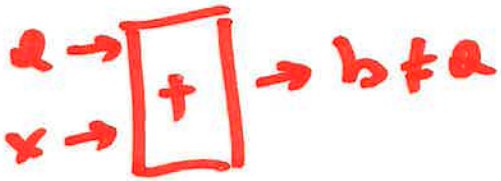
se $\forall x \in X \; \exists y \in X : x * y = y * x = e$

- È ASSOCIATIVA SÉ

$\forall x, y, z \in X : x * (y * z) = (x * y) * z$

$(\mathbb{N} \setminus \{0\}, +)$ $\quad a + b = b + a \quad \forall a, b$ COMMUTATIVA

$a + (b + c) = (a + b) + c$ ASSOCIATIVA



$(\mathbb{N}_0, +)$ $\quad a + 0 = 0 + a = a$ EL. NEUTRO

STRUTT. ALGEBRICA CON EL. NEUTRO, ASSOCIATIVA → MONOIDE

+ COMMUTATIVA → ABELIANO

$(\mathbb{Z}, +)$

GRUPPO

- $\forall a, b \in \mathbb{Z} \quad a + b = b + a$
- $\forall a \in \mathbb{Z}: \quad a + 0 = 0 + a = a$
- $\forall a, b, c \in \mathbb{Z}: \quad (a + b) + c = a + (b + c)$
- esistenza degli inversi: $\forall a \in \mathbb{Z} \; \exists (-a) \in \mathbb{Z}: \quad a + (-a) = 0$

Definisco $a - b := a + (-b)$

$$a - (b - c) = a - b + c \neq (a - b) - c =$$
$$= a - b - c$$

$a - b \neq b - a$

$a - 0 = a$

$0 - a = -a \neq a$ se $a \neq 0$

Def: Si dice gruppo una struttura algebrica $(X, *)$ con X insieme, $* : X \times X \to X$ op. binaria tale che

1) $\exists e \in X : \forall y \in X : \; e * y = y * e = y$
2) $\forall x \in X \; \exists y \in X : \; x * y = y * x = e$
3) $\forall x, y, z \in X : \; x * (y * z) = (x * y) * z$

Esempi $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$

$(\mathbb{C}, +)$.

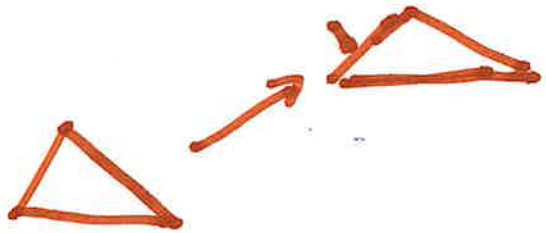
$(\mathbb{Q} \setminus \{0\}, \cdot)$ $\quad \mathbb{K} \setminus \{0\} = \mathbb{K}^*$

$(\mathbb{R} \setminus \{0\}, \cdot)$

$(\mathbb{C} \setminus \{0\}, \cdot)$

- Gruppo delle traslazioni del piano euclideo.

(ABELIANO).



- Gruppo dei movimenti rigidi del piano.

$(\mathbb{Z}, +)$

$(X, *)$

$a * x = b \quad a, b \in X$

$\hat{a}$ = el. inverso di a

$a * x = b$

$\hat{a} * a = e$

$$\hat{a} * (a * x) = \hat{a} * b$$
$$\| $$
$$(\hat{a} * a) * x = \hat{a} * b$$
$$\| $$
$$e * x = \hat{a} * b$$
$$\| $$
$$x = \hat{a} * b$$

sono differenti se il gruppo non è commutativo.

$x * a = b \longrightarrow x = b * \hat{a}$

$(\mathbb{Z}, +)$

$5 + x = 3 \qquad a = 5 \quad b = 3$

$\hat{a} = (-5)$

$(-5) + (5 + x) = (-5) + 3$

$(-5 + 5) + x = -2$

$0 + x = -2$

$x = -2$

$(\mathbb{Q} \setminus \{0\}, \cdot)$

$6x = 7 \qquad a = 6 \quad b = 7$

$\hat{a} = \left(\frac{1}{6}\right)$

$\frac{1}{6}(6x) = \frac{1}{6} \cdot 7$

$\left(\frac{1}{6} \cdot 6\right)x = \frac{7}{6}$

$1 \cdot x = \frac{7}{6} \qquad x = \frac{7}{6}$

$$X = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid (a,b) \neq (0,0) \right\}.$$

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \cdot \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac-bd & ad+bc \\ -bc-ad & ac-bd \end{bmatrix}$$

$(X, \cdot)$ è un gruppo (commutativo).

$$\begin{cases} ac-bd=0 \\ ad+bc=0 \end{cases} \Rightarrow a=b=0 \text{ oppure } c=d=0$$

$$a = \frac{bd}{c} \qquad c \neq 0 \qquad \frac{bd}{c}d + bc = 0$$

$$b(c^2+d^2) = 0$$

$\Rightarrow$ se $(c,d) \neq (0,0)$ $\quad b = 0$

$\Rightarrow \quad ac - bd = 0 \quad \Rightarrow \quad ac = 0$

$c \neq 0 \Rightarrow \quad a = 0$

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} =$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

TROVARE INVERSI + ASSOCIATIVA: Esercizio.

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} x & y \\ -y & x \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

~~$ac - bd = 1$~~

~~$ad + bc = 0$~~

$$\begin{cases} ax - by = 1 \\ ay + bx = 0 \end{cases} \qquad x \neq 0$$

$$a = \frac{1 - by}{x}$$

$$(1 - by)y = -bx^2$$

~~$-b$~~ $\quad y - by^2 + bx^2 = 0 \ldots$

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} a & -b \\ b & a \end{bmatrix} = \begin{bmatrix} a^2+b^2 & -ab+ab \\ +eb-ab & a^2+b^2 \end{bmatrix} = \not{1}$$

$$= \begin{bmatrix} a^2+b^2 & 0 \\ 0 & a^2+b^2 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} \frac{a}{a^2+b^2} & \frac{-b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{bmatrix} \quad e^- \begin{bmatrix} a & b \\ -b & a \end{bmatrix}^{-1}$$

$$(X, \cdot) \quad \approx \quad (\mathbb{C}^*, \cdot)$$

Def. Siano $(G, *)$ ed (H, Δ) due gruppi.
Si dice che $G \cong H$ G <u>isomorfo</u> ad H
se $\exists\ \varphi : G \to H$ funzione tale che

$$\varphi(g_1 * g_2) = \varphi(g_1) \Delta \varphi(g_2)$$

$$\varphi(g_1^{-1}) = \varphi(g_1)^{\nabla -1}$$

e φ biiettiva.

Se φ non invertibile $\Rightarrow$ φ è detta omomorfismo.

$$\varphi \begin{cases} (\mathbb{Z}, +) \longrightarrow (H, \cdot) \\ x \longmapsto \exp(x) \end{cases} \qquad H = \{e^x \mid x \in \mathbb{Z}\}.$$

$\ldots -2, -1, 0, 1 \ldots$ $\qquad \{\ldots e^{-2}, e^{-1}, 1, e \ldots\}.$

$$\varphi(a+b) = e^{a+b} = e^a \cdot e^b = \varphi(a) \cdot \varphi(b)$$

$$\varphi(-a) = e^{-a}$$

$$\varphi(a) \cdot \varphi(-a) = e^{+a} \cdot e^{-a} = e^0 = 1 \Rightarrow$$

$$\Rightarrow \varphi(-a) = \varphi(a)^{-1}$$

é isomorfismo?

1) INIETTIVA

$$\varphi(a) = \varphi(b) \Rightarrow e^a = e^b \Rightarrow$$

$$e^{a-b} = 1 \Rightarrow a-b=0$$

$$a=b$$

2) SURIETTIVA.

$\log: H \to \mathbb{Z}$ è l'inversa di φ.

ATT.: Se φ non è suriettiva si può sempre troncare ad $\mathrm{Im}\,\varphi \Rightarrow$ OTTENIAMO UNA FUNZIONE SURIETTIVA

Se φ NON È INIETTIVA $\Rightarrow$ ⚠

$\ker(\varphi) := \{a \in G : \varphi(a) = 1_H\}$ $\quad \varphi: G \to H.$

↓ nucleo

φ è iniettiva $\iff \ker(\varphi) = \{e_G\}$

inoltre ∃ una corrispondenza biunivoca fra

gli elementi della preimmagine di un $x \in Im(\varphi)$ e $Ker(\varphi)$.

Se $Ker\,\varphi \neq \{1_G\} \Rightarrow 1_H$ ammette più di una preimmagine $\Rightarrow \varphi$ non è iniettiva.

Se no supponiamo

$$\varphi(a) = \varphi(b) = x$$

$$\Rightarrow [\varphi(b)]^{-1}\varphi(a) = x^{-1}\cdot x = 1_H$$

$$\varphi(b^{-1})\cdot\varphi(a) = \varphi(b^{-1}a) = 1_H$$

$b^{-1}a \in \ker(\varphi) \Rightarrow$

$\Rightarrow a \in b^{+1} \cdot \ker(\varphi) =$

$= \{ b^{+1} x \mid x \in \ker(\varphi) \}.$

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

ANELLO CON 1 UNITÀ.

prop distributive.

COMMUTATIVO

$(\mathbb{Z}, +)$ è un gruppo abeliano

$(\mathbb{Z}, \cdot)$ vale

1) $\exists$ el. neutro 1

2) vale la prop. associativa

$a \cdot (b \cdot c) = (a\,b) \cdot c$

$\forall a, b, c \in \mathbb{Z}$: $a \cdot (b+c) = ab + ac$

$(a+b) \cdot c = ac + bc$

$a \cdot b = b \cdot a$

Def: $(W,+,\cdot)$ è detta **anello**

se 1) $(W,+)$ è un gruppo commutativo

2) $\cdot : W \times W \to W$ è associativo

3) Valgono le distributive

$\forall a,b,c \in W : a\cdot(b+c) = a\cdot b + a\cdot c$

$(a+b)\cdot c = ac + bc.$

+ **con unità** se $\exists 1 \in W : \forall x \in W : 1\cdot x = x\cdot 1 = x$

+ **commutativo** se $\forall x,y \in W : x\cdot y = y\cdot x$

+ **dominio di integrità** se $\forall x,y \in W : xy = 0 \Rightarrow x = 0$ oppure $y = 0$.

In un anello: $\forall x \in \Omega : \quad x \cdot 0 = 0 \cdot x = 0$

Dimostrazione

$$x \cdot 0 = x \cdot (0+0) = x \cdot 0 + x \cdot 0$$

$$0 = x \cdot 0 + x \cdot 0$$

$$(-x \cdot 0) + 0 = (-x \cdot 0) + (x \cdot 0 + x \cdot 0)$$

$$0 = [(-x \cdot 0) + (x \cdot 0)] + x \cdot 0$$

$$0 = 0 + x \cdot 0$$

$$0 = x \cdot 0$$

$$\Leftrightarrow \quad x \cdot 0 = 0$$

$$\bar{0} = x \cdot \bar{0} = x \cdot (\alpha + (-\alpha)) = x \cdot \alpha + x \cdot (-\alpha) \quad \Leftrightarrow \quad x \cdot (-\alpha) = -(x \cdot \alpha)$$

Esempio di anello che NON È UN DOMINIO DI INTEGRITÁ $\mathbb{Z}_4$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$2 \cdot 2 = 0$ e $2 \neq 0$

$\mathbb{Z}_5$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbb{Z}[x] = \{ p(x) \mid p \text{ polinomio in } \mathbb{Z} \}$.

$\mathbb{K}[x] = \{ p(x) : p(x) \text{ polinomio a coeff. in } \mathbb{K} \}$.

$$p(x) = \sum_{i=0}^{n} a_i x^i \qquad a_i \in \mathbb{K} \qquad n \geq 0$$

$$\mathbb{K}[x]_{\leq t} := \left\{ \sum_{i=0}^{t} a_i x^i \mid a_i \in \mathbb{K} \right\}$$

polinomi di grado al più t.

$(\mathbb{K}[x], +, \cdot)$ se $\mathbb{K}$ è un anello si può dare una struttura di anello.

$$p(x) + q(x) = (p+q)(x)$$

$$p(x) = \sum a_i x^i \qquad q(x) = \sum b_i x^i$$

$$(p+q)(x) = \sum (a_i + b_i) x^i$$

$$(p \cdot q)(x) = \sum_{i=0}^{t} \sum_{l+m=i} (a_l b_m) x^i$$

con $t = \deg p + \deg q$.

$$\deg p(x) = \max\{i : a_i \neq 0\} \quad \text{se } p(x) \neq 0$$

\ altrimenti: -1

$(\mathbb{Z}, +, \cdot)$ possiamo scrivere l'eq.

$$ax + b = 0$$

in generale in $\mathbb{Z}$ è

$$ax = -b$$

↓

$$ax = b$$

$2x - 4 = 0 \Rightarrow 2x = 4 \Rightarrow x = 2$

Ma $\exists$ altri $\mathbb{Z}$ per cui $2x = 4$?

Se $x \neq 0 \Rightarrow 4 = 0$ IE

Se $x = 0 \Rightarrow 4 \neq 0$ IE

$\forall z \neq 2$

$\forall A$ $z \cdot 0 = 4 \cdot 0 \Rightarrow 0 = 0$

$2x = 3 \qquad \nexists z \in \mathbb{Z}$

$ax + b = 0$ ammette soluzione con $a \neq 0$

se e solamente se $\exists k : b = ak$

cioè b è <u>divisibile per k</u>.

$(\mathbb{K}, +, \cdot)$ è un campo se $(\mathbb{K}, +, \cdot)$ è un anello commutativo con unità e

$(\mathbb{K} \setminus \{0\}, \cdot) = (\mathbb{K}^*, \cdot)$

è un gruppo abeliano.

$(\mathbb{Q}, +, \cdot) \quad (\mathbb{R}, +, \cdot), (\mathbb{C}, \cdot) \quad (\mathbb{Z}_5, +, \cdot)$