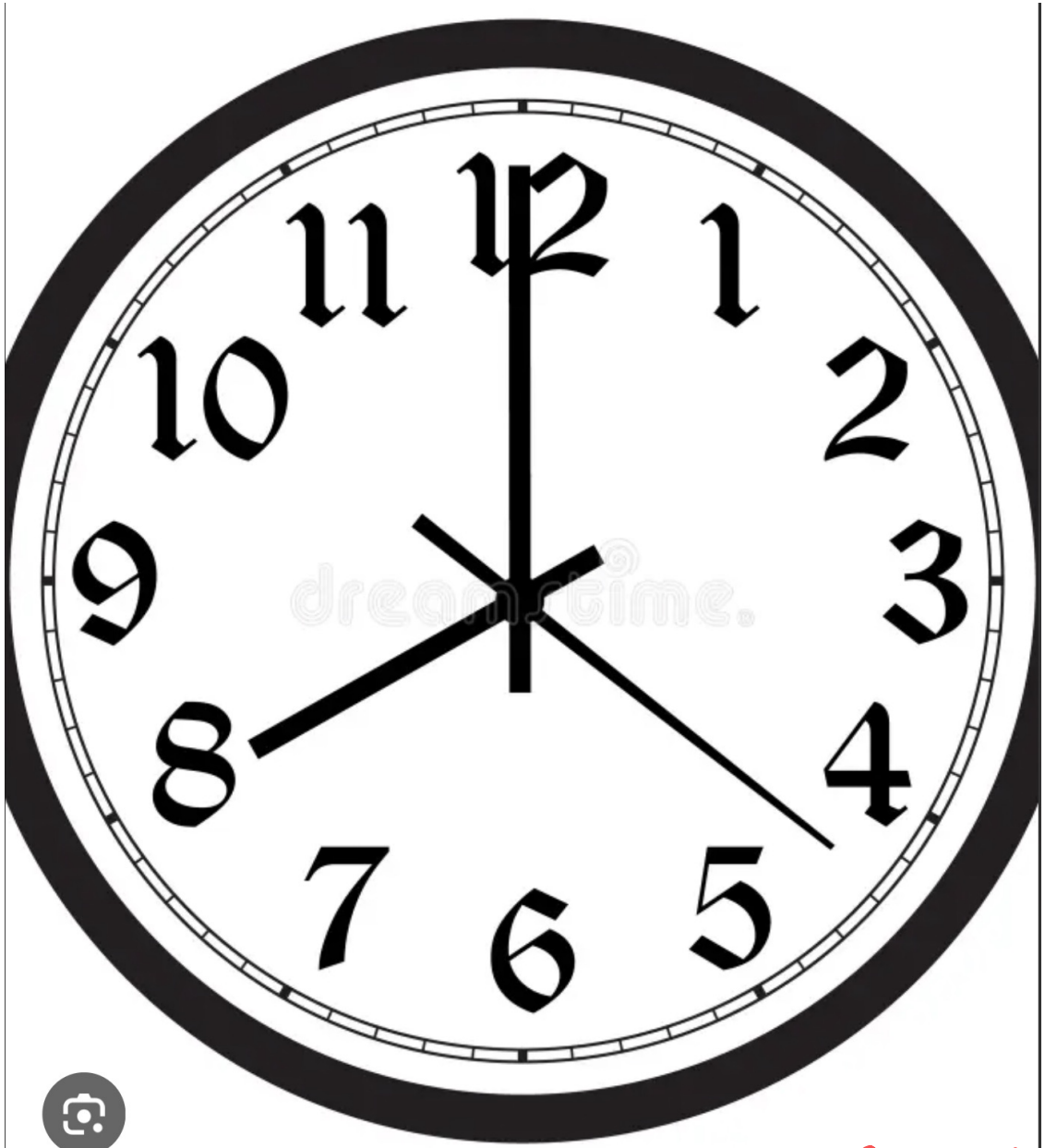
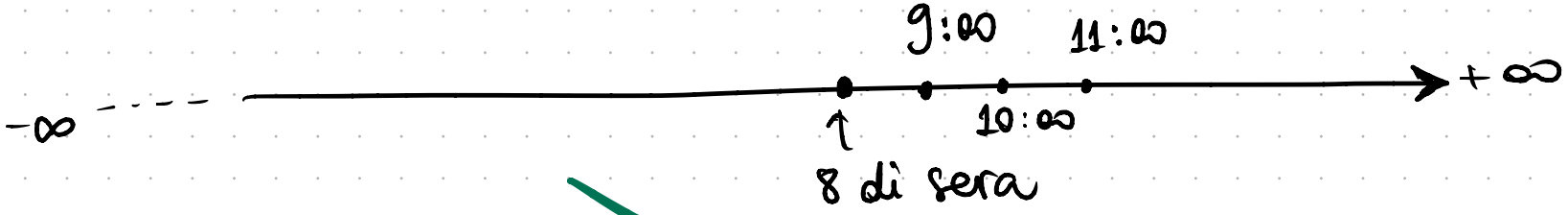
IT'S $\mathbb{Z}_n$ O' CLOCK!



Q: Sono le otto di mattina o le otto di sera?

STEP 1: Prendiamo la linea del tempo



STEP 2: DISCRETIZZIAMOLA TENENDO SOLO LE ORE INTERE

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

ANELLO ABELIANO CHE NON È UN CAMPO

STEP 3:

Scegliamo $n \geq 1$ un numero naturale, e "ripieghiamo" il tempo discreto su di un orologio con n ore.

Formalmente: $\forall a, b \in \mathbb{Z}$

$$a \sim_n b \iff 12 \mid a-b$$

(n = SOSTITUISCO CON UN n QUALSIASI; $\mid$ = DIVIDE)

definisce una RELAZIONE DI EQUIVALENZA!

Esempio: Se sono le 20:00 oppure le 8:00, l'orologio segna la stessa ora. Questo perché $20-8=12$, che è divisibile per 12.

D: Se abbiamo una RELAZ. di EQUIVALENZA, cosa succede se ne prendiamo l'insieme QUOZIENTE?

Def [Anello degli INTERI MODULO n]. Sia $(\mathbb{Z}_n, +, \cdot)$ definito come l'insieme quoziente $\mathbb{Z}_n = \mathbb{Z}/\sim_n$ munito delle operazioni $+$ e $\cdot$ che ora vengono applicate ad uno qualsiasi dei rappresentanti della classe di equivalenza. Quindi:

$$\mathbb{Z}_n = \{[0], [1], [2], [3], \dots, [n-1]\}$$

(ESATTAM. n ELEMENTI)

E SONO I RESTI DELLA DIVISIONE PER n.

Esempio: Prima del quoziente: $7 \cdot 5 = 35$

Dopo il quoziente: $[7] \cdot [5] = [35] = [23] = [11] = [-1]$.

Prima del quoziente: $7 + 5 = 12$

Dopo il quoziente: $[7] + [5] = [12] = [0]$.

Esercizio: Verificare attentamente che scegliendo rappresentanti diversi delle classe d'equivalenza, il risultato della somma e del prodotto non cambia!

Conclusione: $\forall n \geq 1$ $(\mathbb{Z}_n, +, \cdot)$ è ancora un ANELLO ABELIANO.

D: E SE PER ALCUNI VALORI DI n $(\mathbb{Z}_n, +, \cdot)$ FOSSE UN CAMPO?

Esempio: $n = 2$

SI VERIFICA CHE È UN CAMPO

TABELLA della SOMMA

+	0	1
0	0	1
1	1	0

TABELLA della MOLTIPLICAZ.

·	0	1
0	0	0
1	0	1

Esempio: $n=3$

anche per $n=3$ viene fuori un campo

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

RESTO MODULO 3

$2 \cdot 2 = 4 \equiv_3 1$

D: FORSE $(\mathbb{Z}_n, +, \cdot)$ È UN CAMPO PER OGNI $n \geq 1$?

R: IN EFFETTI PER $n=4$ NON È UN CAMPO!

Si può vedere così: $[2] \neq [0]$ in $\mathbb{Z}_4$, però $[2]\cdot[2] = [4] = [0]$

Se per assurdo esistesse l'inverso $[2]^{-1}$ di $[2]$, allora potremmo semplificare l'equazione:

$$\underbrace{[2]^{-1}\cdot[2]}_{=[1]}\cdot[2] = \underbrace{[0]\cdot[2]^{-1}}_{=[0]}$$

ottenendo che

$$[2] = [0],$$

che è un assurdo! Quindi $[2]^{-1}$ NON PUÒ ESISTERE.

Ma in un CAMPO OGNI ELEMENTO DEV'ESSERE INVERTIBILE, e QUINDI $(\mathbb{Z}_4, +, \cdot)$ NON PUÒ ESSERE UN CAMPO!

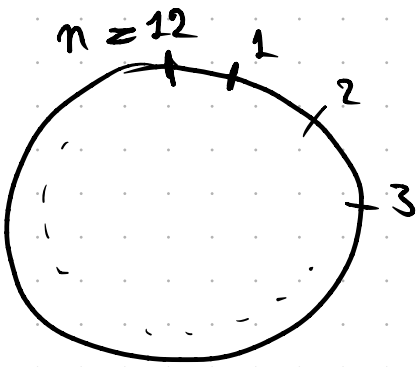
Si potrebbe sospettare che l'essere o meno un CAMPO abbia a che fare con la presenza di questi elementi non nulli che però "DIVIDONO LO ZERO"

Def [DIVISORI dello ZERO]. Sia $(R,+,\cdot)$ un anello. Allora $a \neq 0 \in R$ è un divisore dello zero se $a \cdot b = 0 \in R$ per qualche $0 \neq b \in R$.

Oss Un divisore dello zero NON PUÒ ESSERE INVERTIBILE.
Se lo fosse $a \cdot b = 0 \Rightarrow \underbrace{a^{-1} \cdot a}_{=1} \cdot b = a^{-1} \cdot 0 = 0 \Rightarrow b = 0$
contraddicendo l'ipotesi che b non sia nulla.

Oss Se troviamo divisori dello zero in R, allora NON è un CAMPO!

Esercizio:



$[0] \neq [0]$
$[3] \cdot [4] = [12] = [0]$
$\Rightarrow [3]$ è un DIVISORE DELLO ZERO

D: Per quali n abbiamo divisori dello zero?
Si provi con $n = 1, 2, \ldots, 20$ e si classifichino i casi.

Q: Che ne è invece del viceversa: se in $\mathbb{Z}_n$ non ci sono divisori dello zero, allora è un CAMPO?

[TEOREMA] $\mathbb{Z}_n$ è CAMPO $\iff$ n PRIMO. ← Primo teorema del corso con dimostrazione!

Dimostrazione:

$\Rightarrow$) Dimostriamo che se n NON è PRIMO allora $\mathbb{Z}_n$ NON è un CAMPO. Se n non è primo, allora è composto, quindi $n = a \cdot b$ con a, b divisori propri di n. Allora $[a] \cdot [b] = [n] = [0] \in \mathbb{Z}_n$, quindi $[a]$ è un divisore dello zero, perciò $\mathbb{Z}_n$ non è un campo.
($[a] \neq [0]$, $[b] \neq [0]$)

$\Leftarrow$) È sufficiente dimostrare che ogni elemento è invertibile per la moltiplicazione, perché tutte le altre proprietà del campo per $\mathbb{Z}_n$ sono già viste. Sia $[a] \in \mathbb{Z}_n$. È sufficiente dimostrare che $[a] \cdot [b] = [1] \in \mathbb{Z}_n$ per qualche $[b] \in \mathbb{Z}_n$

Consideriamo $T := \{ [a] \cdot [m] \mid m = 0, 1, \dots, n-1 \}$

Chiaramente T ha al più n elementi. Supponiamo che T abbia meno di n elementi. Allora $[a]\cdot[m_1] = [a]\cdot[m_2]$ per qualche m_1, m_2 tali che $m_1 \neq m_2$, perciò:

$$[a]\underbrace{([m_1]-[m_2])}_{[m_1-m_2]} = \underbrace{[0]}_{\|\ [n]}$$

Però n è PRIMO per ipotesi, quindi n deve dividere a oppure dividere $m_1 - m_2$, che è impossibile. Allora T deve avere esattamente n elementi.

$$\underbrace{T}_{n \text{ ELEMENTI}} \subseteq \underbrace{\{[0],[1],\dots,[n-1]\}}_{n \text{ ELEMENTI}}$$

Per il principio dei piccioni, o dei cassetti, T deve essere UGUALE a TUTTO $\mathbb{Z}_n$! In particolare $[1] \in T$! Ma gli elementi di T sono della forma $[a]\cdot[m]$, quindi $\exists m$:

$[a]\cdot[m] = [1] \in \mathbb{Z}_n \Rightarrow [m] = [a]^{-1} \Rightarrow$ ogni elemento in $\mathbb{Z}_n$ è invertibile $\Rightarrow \mathbb{Z}_n$ è UN CAMPO. □