# Iperreali

## 01 - definizione di un insieme numerico

Liceo scientifico G.B. Grassi di Latina – www.liceograssilatina.org



gualtiero.grassucci@liceograssilatina.org

In collaborazione con le professoresse Annalisa Malusa e Lucilla Galterio

# Il laboratorio



- Tempi: 12 ore comprensive della prova di verifica
- Collegamenti con altri laboratori:
  - **Introduzione al grafico delle funzioni** con gli iperreali nel quarto anno
  - **Introduzione al calcolo integrale** con gli iperreali nel quarto anno
- Per l'introduzione il laboratorio prende spunto dal materiale della professoressa Malusa *Dal naturale al reale*
- L'obiettivo è quello di fornire le conoscenze e le competenze necessarie all'uso del calcolo differenziale già dal terzo anno del liceo

# Il percorso

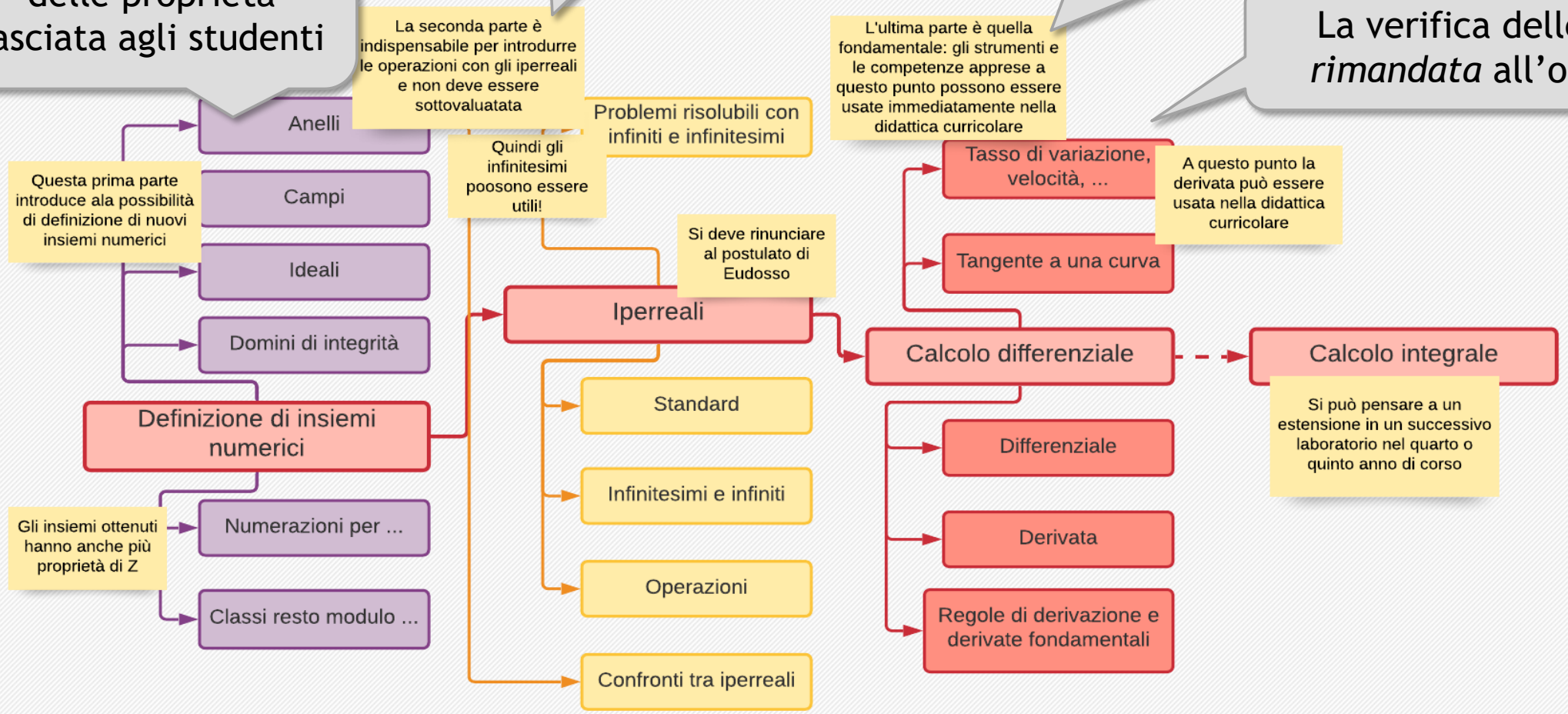


Due ore con verifica delle proprietà lasciata agli studenti

Quattro ore con verifica delle proprietà lasciata agli studenti

Sei ore con *scoperta* di alcune formule di derivazione e di alcune derivate fondamentali (l'applicazione è fondamentalmente lasciata all'orario curricolare)

La verifica delle competenze è *rimandata* all'orario curricolare



# Il percorso



- Il percorso (nel terzo anno)è articolato come segue:
  - La definizione di nuovi insiemi numerici, alcuni esempi (da Valenti, S. - Dall'intero all'iperreale)
  - La definizione dell'insieme degli iperreali. Le operazioni con i numeri iperreali, le proprietà, alcuni problemi risolubili con gli infinitesimi
  - Il calcolo differenziale. Definizione di derivata, significato geometrico e fisico, formule di derivazione principali (tra cui la derivata di una funzione composta), derivate di funzioni polinomiali, razionali fratte e irrazionali
  - Problemi affrontati con il calcolo differenziale. Tangenti, velocità istantanea, tasso di variazione istantaneo
  - Derivate delle funzioni esponenziali e logaritmiche
  - Comportamento asintotico delle funzioni

# L'insieme dei numeri naturali



- Quali proprietà ha l'insieme dei numeri interi $\mathbb{N}$?
- Ha un'operazione detta **somma** $+$ per cui $x + y \epsilon \mathbb{N}\ \forall x, y \epsilon \mathbb{N}$
  - è **commutativa**: $x + y = y + x$
  - è **associativa**: $(x + y) + z = x + (y + z)$
  - è dotata di **elemento neutro** (lo zero) tale che:
  - **non esiste per tutti gli $x$ l'elemento l'opposto** –
- Ha un'operazione detta **moltiplicazione** $\cdot$ per cui $x \cdot y \epsilon \mathbb{N}\ \forall x, y \epsilon \mathbb{N}$
  - è **commutativa**: $x \cdot y = y \cdot x$
  - è **associativa**: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
  - è dotata di **elemento neutro** (l'uno) tale che: $x \cdot 1 = x$
  - **non esiste per tutti gli $x$ l'elemento reciproco $1/x$ tale che: $x \cdot 1/x = 1$**
- La somma $+$ è **distributiva** rispetto alla moltiplicazione $\cdot$:
  - $x \cdot (y + z) = x \cdot y + x \cdot z$

In $\mathbb{N}$ è anche possibile stabilire un ordinamento: si può sempre decidere se $x \geq y$ o $y \geq x$

# L'insieme dei numeri interi



- Quali proprietà ha l'insieme dei numeri interi $\mathbb{Z}$?
- Ha un'operazione detta **somma** $+$ per cui $x + y \epsilon \mathbb{Z}\ \forall x, y \epsilon \mathbb{Z}$
  - è **commutativa**: $x + y = y + x$
  - è **associativa**: $(x + y) + z = x + (y + z)$
  - è dotata di **elemento neutro** (lo zero) tale che: $x + 0 = x$
  - ogni elemento $x$ è dotato dell'**opposto** $-x$ tale che: $x + (-x) = 0$
- Ha un'operazione detta **moltiplicazione** $\cdot$ per cui $x \cdot y \epsilon \mathbb{Z}\ \forall x, y \epsilon \mathbb{Z}$
  - è **commutativa**: $x \cdot y = y \cdot x$
  - è **associativa**: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
  - è dotata di **elemento neutro** (l'uno) tale che: $x \cdot 1 = x$
  - **non esiste per tutti gli $x$ l'elemento reciproco $1/x$ tale che: $x \cdot 1/x = 1$**
- La somma $+$ è **distributiva** rispetto alla moltiplicazione $\cdot$:

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

In $\mathbb{Z}$ è anche possibile stabilire un ordinamento: si può sempre decidere se $x \geq y$ o $y \geq x$

# Anello commutativo con unità



L'insieme degli interi $\mathbb{Z}$ è un anello commutativo con unità, l'insieme dei naturali non lo è!

- Un insieme $A$ è un **anello commutativo con unità** se:

1. In $A$ è definita un'operazione $\oplus$ (addizione) che ad ogni coppia di elementi di $A$ faccia corrispondere un elemento di A (la loro somma)
   - associativa - $a \oplus (c \oplus d) = (a \oplus c) \oplus d$
   - commutativa - $a \oplus b = b \oplus a$
   - con elemento neutro - $a \oplus n = n \oplus a = a$
   - **esistenza dell'opposto** - $a \oplus \bar{a} = \bar{a} \oplus a = n$

Notare che **non è richiesta l'esistenza** dell'opposto (**del reciproco**) per la seconda operazione!

2. In $A$ è definita una seconda operazione $\otimes$ (moltiplicazione) che ad ogni coppia di elementi di $A$ faccia corrispondere un elemento di $A$ (il loro prodotto) associativa e commutativa, con elemento neutro diverso dall'elemento neutro della prima operazione
3. La seconda operazione$\otimes$ sia distributiva rispetto alla prima $\oplus$:

$$a \otimes (c \oplus d) = (a \otimes c) \oplus (a \otimes d)$$

# L'insieme dei numeri razionali



- Quali proprietà ha l'insieme dei numeri razionali $\mathbb{Q}$?
- Ha un'operazione detta **somma** $+$ per cui $x + y \epsilon \mathbb{Q}\ \forall x, y \epsilon \mathbb{Q}$
  - è **commutativa**: $x + y = y + x$
  - è **associativa**: $(x + y) + z = x + (y + z)$
  - è dotata di **elemento neutro** (lo zero) tale che: $x + 0 = x$
  - ogni elemento $x$ è dotato dell'**opposto** $-x$ tale che: $x + (-x) = 0$
- Ha un'operazione detta **moltiplicazione** $\cdot$ per cui $x \cdot y \epsilon \mathbb{Q}\ \forall x, y \epsilon \mathbb{Q}$
  - è **commutativa**: $x \cdot y = y \cdot x$
  - è **associativa**: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
  - è dotata di **elemento neutro** (l'uno) tale che: $x \cdot 1 = x$
  - **esiste per tutti gli $x$ l'elemento reciproco $1/x$ tale che: $x \cdot 1/x = 1$** $\forall x \neq 0$
- La somma $+$ è **distributiva** rispetto alla moltiplicazione $\cdot$:
  - $x \cdot (y + z) = x \cdot y + x \cdot z$

In $\mathbb{Q}$ è anche possibile stabilire un ordinamento: si può sempre decidere se $x \geq y$ o $y \geq x$

Operazione $\otimes$
Proprietà dell'insieme
Reciproco
Nuova notazione
Generalizziamo
Classi resto modulo
Relazioni di equivalenza

# Campo



L'insieme degli interi $\mathbb{Q}$ è un campo!

- Un insieme $A$ è un **campo** se:

1. In $A$ è definita un'operazione $\oplus$ (addizione) che ad ogni coppia di elementi di $A$ faccia corrispondere un elemento di A (la loro somma)
   - associativa - $a \oplus (c \oplus d) = (a \oplus c) \oplus d$
   - commutativa - $a \oplus b = b \oplus a$
   - con elemento neutro - $a \oplus n = n \oplus a = a$
   - esistenza dell'opposto - $a \oplus \bar{a} = \bar{a} \oplus a = n$

Anche la seconda operazione ha qualcosa di simile all'opposto (il reciproco)

2. In $A$ è definita una seconda operazione $\otimes$ (moltiplicazione) che ad ogni coppia di elementi di $A$ faccia corrispondere un elemento di $A$ (il loro prodotto) associativa e commutativa, con elemento neutro $o$ diverso dall'elemento neutro della prima operazione
   - **per ogni elemento $x$** (a eccezione dell'elemento neutro dell'addizione $\oplus$) **esiste un elemento $x^{-1}$ tale che**

$$x \cdot x^{-1} = n$$

3. La seconda operazione$\otimes$ sia distributiva rispetto alla prima $\oplus$:

$$a \otimes (c \oplus d) = (a \otimes c) \oplus (a \otimes d)$$

# Anelli e campi a confronto (1)



| Operazione | Proprietà | Anello | Campo |
|---|---|---|---|
| $\oplus$ | Associativa | | |
| | Commutativa | | |
| | Elemento neutro | | |
| | Opposto | | |
| $\otimes$ | Associativa | | |
| | Commutativa | | |
| | Elemento neutro | | |
| | Opposto | | |
| $\oplus$ distributiva rispetto a $\otimes$ | | | |

# Anelli e campi a confronto (2)



| Operazione | Proprietà | Anello | Campo |
|---|---|---|---|
| $\oplus$ | Associativa | 👍 | 👍 |
| | Commutativa | 👍 | 👍 |
| | Elemento neutro | 👍 | 👍 |
| | Opposto | 👍 | 👍 |
| $\otimes$ | Associativa | 👍 | 👍 |
| | Commutativa | 👍 | 👍 |
| | Elemento neutro | 👍 | 👍 |
| | Opposto | | 👍 |
| $\oplus$ distributiva rispetto a $\otimes$ | | 👍 | 👍 |

# Un nostro insieme numerico (1)

Una **partizione** di $A$ è una suddivisione che copre $A$ senza che gli elementi della partizione si sovrappongano!

- Partiamo dall'insieme $\mathbb{Z}$ dei numeri interi e consideriamo alcune *numerazioni per 3*:
  - $I_3 = \{\dots, -3,\ 0,\ 3,\ 6,\ 9, \dots\}$
  - $Z_1 = \{\dots, -5,\ -2,\ 1,\ 4,\ 7, \dots\}$
  - $Z_2 = \{\dots, -4,\ -1,\ 2,\ 5,\ 8, \dots\}$
- Qualche curiosità:
  - Esistono altre numerazioni per tre?
  - I tre insiemi hanno qualche elemento in comune?
  - C'è qualche elemento di $\mathbb{Z}$ che non è nei tre insiemi che abbiamo scelto?
- Usiamo una notazione più semplice: $Z_1 = u$, $Z_2 = a$ e $I_3 = o$, il nostro insieme è composto dalle tre numerazioni: $H_3 = \{o, u, a\}$

Possiamo definire un ordinamento: $x \geq y$ se il più piccolo intero positivo o nullo in $x$ è maggiore o uguale al più piccolo intero positivo in $y$.
In questo modo $o < u < a$

# Un nostro insieme: operazioni $\oplus$



- Definiamo un'operazione di **addizione** $\oplus$ su $H_3$ in modo che $x \oplus y$ sia la somma (intesa come somma di interi) di ogni elemento di $x$ con tutti gli elementi di $y$, $\forall x, y \in H_3$ inserendo nell'insieme somma un solo elemento per addizioni con lo stesso risultato (insomma … *evitando le ripetizioni*)
- Quali sono le proprietà di $\oplus$?
  - Commutativa?
  - Associativa?
  - Esiste un elemento neutro per l'addizione $\oplus$?
  - Esiste l'opposto di ogni elemento?

Usiamo il simbolo $\oplus$ per ricordare che non si tratta dell'addizione classica tra interi

# Un nostro insieme: operazioni ⊕



- Costruiamo una tabella per l'addizione ⊕ …

| ⊕ | o | u | a |
|---|---|---|---|
| o | | | |
| u | | | |
| a | | | |

| ⊗ | o | u | a |
|---|---|---|---|
| o | | | |
| u | | | |
| a | | | |

# Un nostro insieme: operazioni ⊕



- Costruiamo una tabella per l'addizione ⊕ …

| ⊕ | o | u | a |
|---|---|---|---|
| o | o | u | a |
| u | u | a | o |
| a | a | o | u |

| ⊗ | o | u | a |
|---|---|---|---|
| o | | | |
| u | | | |
| a | | | |

La tabella rende più facile la verifica delle proprietà. Per esempio, ⊕ è commutativa se la tabella è simmetrica rispetto alla diagonale principale!

# Un nostro insieme: operazioni $\otimes$



- Definiamo un'operazione di **moltiplicazione** $\otimes$ su $H_3$ in modo che $x \otimes y$ sia il prodotto (inteso come prodotto di interi) di ogni elemento di $x$ con tutti gli elementi di $y$, $\forall x, y \in \tilde{A}$ inserendo nell'insieme prodotto un solo elemento per moltiplicazioni con lo stesso risultato (insomma … evitando le ripetizioni)
- Quali sono le nuove proprietà di $\otimes$?
  - Commutativa?
  - Associativa?
  - Esiste un elemento neutro per la moltiplicazione $\otimes$? E l'opposto di ogni elemento?
  - L'addizione $\oplus$ è distributiva rispetto alla moltiplicazione $\otimes$?
- E le proprietà di $H_3$?
  - È un anello? È un campo?
  - È un dominio di integrità?

Usiamo il simbolo $\otimes$ per ricordare che non si tratta della moltiplicazione classica tra interi

# Un nostro insieme: operazioni ⊗



- Costruiamo una tabella per la moltiplicazione ⊗ …

| ⊕ | o | u | a |
|---|---|---|---|
| o | o | u | a |
| u | u | a | o |
| a | a | o | u |

| ⊗ | o | u | a |
|---|---|---|---|
| o | | | |
| u | | | |
| a | | | |

# Un nostro insieme: operazioni ⊗



- Costruiamo una tabella per la moltiplicazione ⊗ …

| ⊕ | o | u | a |
|---|---|---|---|
| o | o | u | a |
| u | u | a | o |
| a | a | o | u |

| ⊗ | o | u | a |
|---|---|---|---|
| o | o | o | o |
| u | o | u | a |
| a | o | a | u |

La distributività può anche essere verificata provando tutte le possibili combinazioni $x \otimes (y \oplus z)$ con $x, y, z \in H_3$ (e ricordando che le due operazioni sono commutative)

# Il nostro insieme numerico (2a)



| Operazione | Proprietà | Anello | Campo | $\tilde{A}$ |
|---|---|---|---|---|
| $\oplus$ | Associativa | 👍 | 👍 | |
| | Commutativa | 👍 | 👍 | |
| | Elemento neutro | 👍 | 👍 | |
| | Opposto | 👍 | 👍 | |
| $\otimes$ | Associativa | 👍 | 👍 | |
| | Commutativa | 👍 | 👍 | |
| | Elemento neutro | 👍 | 👍 | |
| | Opposto | | 👍 | |
| $\oplus$ distributiva rispetto a $\otimes$ | | 👍 | 👍 | |

# Il nostro insieme numerico (2b)



| Operazione | Proprietà | Anello | Campo | $\tilde{A}$ |
|---|---|---|---|---|
| $\oplus$ | Associativa | 👍 | 👍 | 👍 |
| | Commutativa | 👍 | 👍 | 👍 |
| | Elemento neutro | 👍 | 👍 | 👍 |
| | Opposto | 👍 | 👍 | 👍 |
| $\otimes$ | Associativa | 👍 | 👍 | 👍 |
| | Commutativa | 👍 | 👍 | 👍 |
| | Elemento neutro | 👍 | 👍 | 👍 |
| | Opposto | | 👍 | 👍 |
| $\oplus$ distributiva rispetto a $\otimes$ | | 👍 | 👍 | 👍 |

# Reciproco



- L'inverso (il reciproco) $a^{-1} \epsilon H_3$ di un elemento $a \epsilon H_3$ ha la proprietà che

$$a \otimes a^{-1} \epsilon H_3$$

- Tutti gli elementi di $H_3$ a eccezione dello $\bar{0}$ hanno un inverso (notare che in $\mathbb{Z}$ solo alcuni elementi hanno l'inverso)

**Quindi $A_3$ è un campo (ma $\mathbb{Z}$ non lo è)**

La presenza del reciproco permette l'introduzione di una nuova operazione: la **divisione**!

Curioso: il nostro insieme numerico è costruito a partire dagli interi ma ha più proprietà dell'insieme *genitore!*

# Il nostro insieme numerico (3)



- $H_3 = \{o, u, a\}$ con $o$, $u$ e $a$ definiti in precedenza

**è un anello commutativo con unità**

$A_3$ è dotato anche di un ordinamento!

- le cui operazioni $\oplus$ e $\otimes$ sono quelle definite prima
- è naturale guardare quei tre oggetti come nuovi numeri, dal momento che fra essi risulta definito un ben preciso calcolo algebrico
- le regole di questo calcolo possono totalmente prescindere dalla natura intrinseca di $o, u, a$:

**si applicano anche senza tenere in alcun conto il fatto che i tre oggetti siano in realtà tre insiemi di numeri interi**

# Cambiamo ancora notazione



- Poniamo $o \sim \bar{0}$, $u \sim \bar{1}$ e $a \sim \bar{2}$
- Il nostro insieme diventa $H_3 = \{\bar{0}, \bar{1}, \bar{2}\}$
- La nuova notazione è, in un certo senso, naturale: $\bar{0}$ è l'elemento neutro dell'addizione $\oplus$, $\bar{1}$ è l'elemento neutro della moltiplicazione $\otimes$

| $\oplus$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{0}$ | $\bar{1}$ |

| $\otimes$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{1}$ |

Notare che ora le operazioni sembrano *naturali*

# Generalizzazione (1)



- Per costruire il nostro insieme numerico $H_3$ abbiamo:
  - Ripartito $\mathbb{Z}$ in tre insiemi $o, u, a$ (i tre insiemi non hanno elementi in comune e ogni elemento di $\mathbb{Z}$ appartiene a uno dei tre sottoinsiemi)
  - Abbiamo definito un'operazione di addizione e verificato le proprietà
  - Abbiamo definito un'operazione di moltiplicazione e verificato le proprietà
- I tre *oggetti* $o, u, a$ sono a tutti gli effetti dei **numeri**
- Cosa succede se proviamo a sviluppare, con lo stesso procedimento, insiemi numerici a partire dalle numerazioni per 4, 5, 6, 7, 8, 9, 10, 11?
- I nuovi insiemi numerici (alcuni, tutti, …) hanno le stesse proprietà di $H_3$? Perché?

# Generalizzazione (2)



- Il processo si può utilizzare per costruire nuovi insiemi numerici
  - P.es.: dalle numerazioni per quattro otteniamo $H_4 = \{o, u, a, b\}$
    - le operazioni hanno tutte le proprietà elencate a eccezione dell'esistenza del reciproco per tutti gli elementi di $H_4$: $H_4$ è un anello commutativo con unità ma non un campo
  - Dalle numerazioni per cinque si ha $H_5 = \{o, u, a, b, c\}$
    - ha tutte le proprietà di $H_4$ ma in più esiste il reciproco per ogni elemento
- Analizzando tutti i possibili casi si deduce che $H_n$ è sempre un anello commutativo con unità ma …

**è un campo sono se $n$ è un numero primo**

# Numerazioni per cinque



- Ripetiamo il procedimento a partire dalle numerazioni per 5
- Sia $o = \{-5, 0, 5, 10, \dots\}$, $u = \{-4, 1, 6, 11, \dots\}$, $a = \{-3, 2, 7, 12, \dots\}$, …

| $\oplus$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |
|---|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |
| $\overline{1}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{0}$ |
| $\overline{2}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{0}$ | $\overline{1}$ |
| $\overline{3}$ | $\overline{3}$ | $\overline{4}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ |
| $\overline{4}$ | $\overline{4}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |

| $\otimes$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |
|---|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ |
| $\overline{1}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |
| $\overline{2}$ | $\overline{0}$ | $\overline{2}$ | $\overline{4}$ | $\overline{1}$ | $\overline{3}$ |
| $\overline{3}$ | $\overline{0}$ | $\overline{3}$ | $\overline{1}$ | $\overline{4}$ | $\overline{2}$ |
| $\overline{4}$ | $\overline{0}$ | $\overline{4}$ | $\overline{3}$ | $\overline{2}$ | $\overline{1}$ |

Ogni elemento ha il reciproco: basta controllare che su ogni riga ci sia l'elemento neutro della $\otimes$, il reciproco è l'elemento che si trova sull'intestazione della colonna corrispondente

# Numerazioni per sei



- Questa volta a partire dalle numerazioni per 6
- Sia $o = \{-6, 0, 6, 12, \dots\}$, $u = \{-5, 1, 7, 13, \dots\}$, $a = \{-4, 2, 8, 14, \dots\}$, …

| $\oplus$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ |
|---|---|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ |
| $\overline{1}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ | $\overline{0}$ |
| $\overline{2}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ | $\overline{0}$ | $\overline{1}$ |
| $\overline{3}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ |
| $\overline{4}$ | $\overline{4}$ | $\overline{5}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |
| $\overline{5}$ | $\overline{5}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |

| $\otimes$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ |
|---|---|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ |
| $\overline{1}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ |
| $\overline{2}$ | $\overline{0}$ | $\overline{2}$ | $\overline{4}$ | $\overline{0}$ | $\overline{2}$ | $\overline{4}$ |
| $\overline{3}$ | $\overline{0}$ | $\overline{3}$ | $\overline{0}$ | $\overline{3}$ | $\overline{0}$ | $\overline{3}$ |
| $\overline{4}$ | $\overline{0}$ | $\overline{4}$ | $\overline{2}$ | $\overline{0}$ | $\overline{4}$ | $\overline{2}$ |
| $\overline{5}$ | $\overline{0}$ | $\overline{5}$ | $\overline{4}$ | $\overline{3}$ | $\overline{2}$ | $\overline{1}$ |

Non tutti gli elementi hanno il reciproco: notare che sono nelle righe in cui il prodotto è nullo anche se i due operandi sono non nulli!

# Generalizzazione (3)



- Gli insiemi $H_n$ con $n$ primo sono campi: per ogni elemento esiste il reciproco
- Gli insiemi $H_n$ con $n$ non primo sono *solo* anelli commutativi con unità:
  - se alcuni prodotti $x \otimes y$ sono nulli quando nessuno dei due operandi è nullo allora $x$ e $y$ non hanno il reciproco, infatti se esistessero $x^{-1}$ e $y^{-1}$ allora:
  - $x \otimes y = \mathrm{o}$ ma moltiplicando $x^{-1} \otimes x \otimes y \otimes y^{-1} = x^{-1} \otimes o \otimes y^{-1}$
  - da cui $u \otimes u = o$ che è chiaramente una contraddizione
- Ma un prodotto è nullo solo se $x \otimes y = n$ ma questo è impossibile se $n$ è primo

Attenzione: il viceversa non è vero, non è detto che **se un elemento $x$ non ha il reciproco** allora **esiste un prodotto $x \otimes y = o$** con $y$ non nullo

Numeri naturali
Numeri interi
Anello con unità
Numeri razionali
Campo
Insieme numerico
Operazione $\oplus$

Un primo $p$ è scomponibile solo come $p = 1 \cdot p$

# Aritmetica modulare (1)



- **Modulo $mod$** è un'operazione definita tra due interi $a, b \in \mathbb{Z}$ che restituisce il resto della divisione di $a$ per $b$
  - in altre parole, $r = a \; mod \; b$ se per qualche $d \in \mathbb{Z}$ si ha $a = d \cdot b + r$
- Definiamo la **congruenza modulo $n$** come segue: $a$ è congruente a $b$ modulo $n$ se $a - b$ è un multiplo di $n$: $a \equiv b \pmod{n}$.
- La congruenza definisce in $\mathbb{Z}$ una relazione di equivalenza ed è possibile l'insieme degli interi in $n$ classi (sottoinsiemi) con la regola:
  - un intero $a$ è **equivalente** a $b$ modulo $n$ se $a - b$ è un multiplo di $n$: $a \equiv b \pmod{n}$
    Le classi così ottenute si chiamano **classi resto modulo**



In pratica: due elementi $a, b$ sono congruenti se il resto della loro divisione per $n$ è lo stesso!

# Relazione di equivalenza



- Dato un insieme $A$:
  - Una **relazione** tra gli elementi di $A$ è un sottoinsieme $R$ del prodotto cartesiano $\mathrm{R} = A \times A$ e $x\ R\ y$ se $(x, y) \epsilon R$
- Una **relazione di equivalenza** $\sim$ è una relazione:
  - **riflessiva**: $x \sim x\ \forall x \epsilon A$
  - **simmetrica**: se $x \sim y$ allora $y \sim x\ \forall x, y \epsilon A$
  - **transitiva**: se $x \sim y$ e $y \sim z$ allora $x \sim z\ \forall x, y, z \epsilon A$
- Un sottoinsieme di $A$ che contiene tutti gli elementi tra loro equivalenti si chiama **classe di equivalenza**
- L'insieme delle classi di equivalenza è l'**insieme quoziente** ed è una partizione di $A$



Una **partizione** di $A$ è una suddivisione che copre $A$ senza che gli elementi della partizione si sovrappongano!

# Aritmetica modulare (2)



- Costruiamo una tabella delle operazioni + e × per l'insieme delle classi modulo resto 3

| + | 0 | 1 | 2 |
|---|---|---|---|
| 0 | | | |
| 1 | | | |
| 2 | | | |

| × | 0 | 1 | 2 |
|---|---|---|---|
| 0 | | | |
| 1 | | | |
| 2 | | | |

# Aritmetica modulare (2)



- Costruiamo una tabella delle operazioni + e × per l'insieme delle classi modulo resto 3

| $\oplus$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

| $\otimes$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

L'insieme delle classi resto modulo 3 è esattamente l'insieme $H_3$ definito in precedenza!

# Una spiegazione



- Riprendiamo l'affermazione fatta in precedenza:

**$H_n$ è un campo sono se $n$ è un numero primo**

- Se $n$ non è primo in $H_n$ esistono elementi il cui prodotto è nullo anche se i due elementi sono non nulli
  - P.es.: in $H_4$ $\overline{2}x\overline{2} = \overline{0}$
- Per questi elementi non può esistere il reciproco!

**Questa cosa non succede mai se $n$ è primo!**

# Bibliografia




- Goldoni, G. – *I numeri iperreali*– 2017, Ilmiolibro)
- Robinson, A. - *Non standard analysis – 1996, Priceton University Press*
- Stecca, B. & Zambelli, D. – *Analisi non standard* – 2015, docplayer.it/4477695-Analisi-non-standard-release-0-0-1-b-stecca-d-zambelli.html
- Valenti, S. – *Dall'intero all'iperreale, un'introduzione graduata all'analisi non standard* – 1994, GRIM - quaderni di ricerca didattica n.5