

# Lezione 9

Alessandro Ardizzoni

# Costruzione dei numeri interi

Abbiamo indicato in genere con  $\mathcal{R}$  le relazioni d'equivalenza.

Si possono però usare altri simboli.

Uno dei più usuali è  $\sim$  che verrà usato nelle prossime costruzioni.

Vogliamo innanzitutto vedere come si possa costruire  $\mathbb{Z}$  a partire da  $\mathbb{N}$  attraverso gli strumenti che abbiamo introdotto.

Consideriamo sull'insieme  $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$  la relazione  $\sim$  definita ponendo

$$(a, b) \sim (a', b') \Leftrightarrow a + b' = a' + b. \quad \left\| \begin{array}{l} \text{a posteriori} \\ a - b = a' - b' \end{array} \right.$$

## Lemma

*La relazione appena definita è una relazione d'equivalenza su  $\mathbb{N}^2$ .*

DIMOSTRAZIONE. La riflessiva e la simmetrica sono ovviamente soddisfatte. Per la transitività, supponendo  $(a, b) \sim (a', b')$  e  $(a', b') \sim (a'', b'')$  otteniamo  $a + b' = a' + b$  e  $a' + b'' = a'' + b'$ . Ma allora  $a + \cancel{b'} + b'' = a' + b + b'' = a' + b'' + b = \cancel{a'' + b'} + b$ . Semplificando  $b'$  otteniamo  $a + b'' = a'' + b$ , vale a dire  $(a, b) \sim (a'', b'')$ .

## Definizione

L'insieme dei numeri interi è l'insieme quoziente

$$\mathbb{Z} := \mathbb{N}^2 / \sim.$$

Indichiamo al solito la classe di equivalenza di un elemento  $(a, b) \in \mathbb{N}^2$  barrandolo:  $\overline{(a, b)} = \{(a', b') \in \mathbb{N}^2 \mid (a', b') \sim (a, b)\}.$

Cerchiamo di descriverlo meglio. Per farlo, prima definiamo su  $\mathbb{N}$  la relazione d'ordine  $\leq$  ponendo  $a \leq b \Leftrightarrow \exists n \in \mathbb{N}, a + n = b$ . E' chiaro che  $0 \leq 1 \leq 2 \leq 3 \leq \dots$  e che  $(\mathbb{N}, \leq)$  è totalmente ordinato.

non è definita la  
sottrazione in  $\mathbb{N}$ , ma  
solo in  $\mathbb{Z}$

## Osservazione

Consideriamo una coppia  $(a, b) \in \mathbb{N}^2$ .

- Se  $a \geq b$ , esiste  $m \in \mathbb{N}$  tale che  $a = b + m$ . Ma allora  $(a, b) \sim (m, 0)$ .
- Se  $a \leq b$ , esiste  $n \in \mathbb{N}$  tale che  $a + n = b$ . Ma allora  $(a, b) \sim (0, n)$ .
- Siano  $m, n \in \mathbb{N}$  tali che  $(m, 0) \sim (0, n)$ . Allora  $m + n = 0$  il che è possibile solo se  $m = 0 = n$ .

$$\overline{(a, b)} = \overline{(m, 0)}$$



Per l'Osservazione precedente, abbiamo  $(a, b) \sim (m, 0)$  oppure  $(a, b) \sim (0, n)$  e quindi  $\overline{(a, b)} = \overline{(m, 0)}$  oppure  $\overline{(a, b)} = \overline{(0, n)}$ .

Possiamo allora riscrivere  $\mathbb{Z}$  : come

$$\begin{aligned}\mathbb{Z} &= \mathbb{N}^2 / \sim \\ &= \{\overline{(a, b)} \mid a, b \in \mathbb{N}\} \\ &= \{\dots, \overline{(0, 3)}, \overline{(0, 2)}, \overline{(0, 1)}, \overline{(0, 0)}, \overline{(1, 0)}, \overline{(2, 0)}, \overline{(3, 0)}, \dots\}.\end{aligned}$$

Nell'insieme  $\mathbb{Z}$  appena costruito definiamo le operazioni di addizione e moltiplicazione come segue. Per ogni  $\overline{(m, n)}, \overline{(p, q)} \in \mathbb{Z}$  poniamo

$$\overline{(m, n)} + \overline{(p, q)} = \overline{(m + p, n + q)} \quad (\text{somma}),$$

$$\overline{(m, n)} \cdot \overline{(p, q)} = \overline{(mp + nq, mq + np)} \quad (\text{prodotto}).$$

Poiché le operazioni sono state definite mediante dei rappresentanti arbitrariamente scelti occorre verificare che esse siano ben definite.

## Lemma

*L'addizione e la moltiplicazione in  $\mathbb{Z}$  sono ben definite.*

DIMOSTRAZIONE. Vogliamo che l'addizione

$$+ : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, ((\overline{m, n}), (\overline{p, q})) \mapsto \overline{m + p, n + q}$$

sia una funzione. Pertanto dobbiamo mostrare che al cambiare dei rappresentanti non cambia il risultato cioè che

$$((\overline{m, n}), (\overline{p, q})) = ((\overline{m', n'}), (\overline{p', q'})) \Rightarrow \overline{m + p, n + q} = \overline{m' + p', n' + q'}$$

L'uguaglianza di sinistra implica  $\overline{m, n} = \overline{m', n'}$  e  $\overline{p, q} = \overline{p', q'}$  cioè

$$m + n' = m' + n \quad \text{e} \quad p + q' = p' + q.$$

Usando queste uguaglianze otteniamo

$$m + p + n' + q' = m + n' + p + q' = m' + n + p' + q = m' + p' + n + q$$

da cui risulta  $\overline{m + p, n + q} = \overline{m' + p', n' + q'}$ .

Vediamo ora che la moltiplicazione

$$\cdot : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, ((m, n), (p, q)) \mapsto (mp + nq, mq + np)$$

è una funzione.

Di nuovo dobbiamo mostrare che al cambiare dei rappresentanti non cambia il risultato cioè che

$$((m, n), (p, q)) = ((m', n'), (p', q')) \Rightarrow (mp + nq, mq + np) = (m'p' + n'q', m'q' + n'p').$$

L'uguaglianza di sinistra implica come prima

$$m + n' = m' + n \quad \text{e} \quad p + q' = p' + q. \quad (1)$$

L'uguaglianza di destra, che dobbiamo ottenere, è

$$m'q' + n'p' + mp + nq = mq + np + m'p' + n'q'.$$

Si arriva all'uguaglianza cercata sommando al suo primo membro  $m(p' + q) + n(p + q')$  e al secondo membro  $m(p + q') + n(p' + q)$  (si noti che per (1) le quantità sommate sono uguali) e cancellando, dopo qualche manipolazione, tutti i termini usando ancora (1).

L'insieme  $\mathbb{Z}$  dei numeri interi con le sue operazioni è un'estensione dei numeri naturali nel senso della proposizione seguente

### Proposizione (Immersione di $\mathbb{N}$ in $\mathbb{Z}$ )

La funzione

$$\iota : \mathbb{N} \rightarrow \mathbb{Z}, \quad n \mapsto \overline{(n, 0)},$$

è iniettiva e rispetta le operazioni di addizione e moltiplicazione, cioè

$$\forall m, n \in \mathbb{N}, \quad \iota(m+n) = \iota(m) + \iota(n), \quad \iota(mn) = \iota(m) \cdot \iota(n).$$

DIMOSTRAZIONE. Ricordiamo che su  $\mathbb{Z}$  abbiamo definito

$$\overline{(m, n)} + \overline{(p, q)} = \overline{(m+p, n+q)}, \quad \overline{(m, n)} \cdot \overline{(p, q)} = \overline{(mp+nq, mq+np)}.$$

Se  $\iota(m) = \iota(n)$ , allora  $\overline{(m, 0)} = \overline{(n, 0)}$ , cioè  $m+0 = n+0$  da cui  $m = n$ .  
Inoltre, per ogni  $m, n \in \mathbb{N}$ .

$$\iota(m) + \iota(n) = \overline{(m, 0)} + \overline{(n, 0)} = \overline{(m+n, 0)} = \iota(m+n),$$

$$\iota(m) \cdot \iota(n) = \overline{(m, 0)} \cdot \overline{(n, 0)} = \overline{(mn, 0)} = \iota(mn). \quad \square$$

Ora è facile dimostrare, usando come essa è definita, che in  $\mathbb{Z}$

- l'addizione è associativa, commutativa,
- che  $\overline{(0,0)}$  è lo zero (l'elemento neutro in notazione additiva) e che
- $\overline{(n,m)}$  è un opposto di  $\overline{(m,n)}$ .

Vediamo ad esempio quest'ultima proprietà:

$$\overline{(n,m)} + \overline{(m,n)} = \overline{(n+m, m+n)} = \overline{(m+n, m+n)} = \overline{(0,0)}.$$

$-(\overline{(n,m)}) := \overline{(m,n)}$

L'opposto di  $\overline{(n,m)}$  si indica anche con il simbolo  $-(\overline{(n,m)})$  (come si fa solitamente in notazione additiva). Notiamo che  $-\iota(n) = -\overline{(n,0)} = \overline{(0,n)}$ . Pertanto

$$\begin{aligned}\mathbb{Z} &= \{ \dots, \overline{(0,3)}, \overline{(0,2)}, \overline{(0,1)}, \overline{(0,0)}, \overline{(1,0)}, \overline{(2,0)}, \overline{(3,0)}, \dots \} \\ &= \{ \dots, -\iota(3), -\iota(2), -\iota(1), \iota(0), \iota(1), \iota(2), \iota(3), \dots \}\end{aligned}$$

Inoltre per  $\mathbb{Z}$  si può dimostrare che la moltiplicazione è associativa, commutativa, che  $\overline{(1,0)}$  è un elemento neutro e che  $\overline{(m,n)}$  è invertibile solo se  $\overline{(m,n)} = \pm \overline{(1,0)}$  (basta ricordare che  $\overline{(m,n)}$  può essere riscritto in modo che la prima o la seconda entrata della coppia sia nulla).



Alla luce della discussione svolta finora possiamo d'ora in poi adottare la comoda notazione seguente. In luogo l'elemento  $\iota(n) = \overline{(n, 0)}$  scriveremo semplicemente  $n$ . Dunque possiamo riscrivere  $\mathbb{Z}$  nel modo più familiare

$$\begin{aligned}\mathbb{Z} &= \{ \dots, \underbrace{-\iota(3)}_{-3}, \underbrace{-\iota(2)}_{-2}, \underbrace{-\iota(1)}_{-1}, \underbrace{\iota(0)}_0, \underbrace{\iota(1)}_1, \underbrace{\iota(2)}_2, \underbrace{\iota(3)}_3, \dots \} \\ &= \{ \dots, -3, -2, -1, 0, 1, 2, 3, \dots \}.\end{aligned}$$

Con queste notazioni

$$\begin{aligned}m - n &= \iota(m) - \iota(n) \\ &= \overline{(m, 0)} - \overline{(n, 0)} \\ &= \overline{(m, 0)} + (-\overline{(n, 0)}) \\ &= \overline{(m, 0)} + \overline{(0, n)} = \overline{(m, n)}.\end{aligned}$$

## Osservazione

Altre proprietà di  $\mathbb{N}$  vengono ereditate da  $\mathbb{Z}$ . Ad esempio la legge di cancellazione. Se  $\overline{(m, n)} + \overline{(a, b)} = \overline{(m', n')} + \overline{(a, b)}$ , allora  $\overline{(m + a, n + b)} = \overline{(m' + a, n' + b)}$  da cui  $m + a + n' + b = m' + a + n + b$  e cioè

$$m + n' + a + b = m' + n + a + b.$$

Siccome questa è un'uguaglianza in  $\mathbb{N}$  dove la cancellazione vale, otteniamo  $m + n' = m' + n$  il che vuol dire  $\overline{(m, n)} = \overline{(m', n')}$ .

## Esercizio (per casa)

Dimostrare le seguenti proprietà di  $\mathbb{Z}$ .

- Se  $x, y \in \mathbb{Z}$ ,  $x \cdot y = 0 \Rightarrow x = 0 \vee y = 0$  (legge di annullamento del prodotto).
- Definiamo  $\overline{(m, n)} \leq \overline{(m', n')} \Leftrightarrow m + n' \leq m' + n$ . Dimostrare che quello appena definito è un ordine totale su  $\mathbb{Z}$ .
- Se  $x, y \in \mathbb{Z}$  dimostrare che  $x \leq y \Rightarrow -y \leq -x$  (dove la relazione d'ordine è quella del punto precedente).

# Costruzione dei numeri razionali

La costruzione di  $\mathbb{Q}$  a partire da  $\mathbb{Z}$  è simile a quella di  $\mathbb{Z}$  a partire da  $\mathbb{N}$ , per cui daremo indicazione dei passi e delle proprietà fondamentali lasciandone spesso per esercizio la verifica.

Iniziamo considerando la relazione  $\sim$  sull'insieme  $A = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$  definita da

$$(a, b) \sim (a', b') \iff ab' = a'b.$$

Si vede che si tratta di una relazione d'equivalenza su  $A$ . Possiamo ora dare la definizione seguente.

## Definizione

Si dice **insieme dei numeri razionali** l'insieme quoziente

$$\mathbb{Q} := (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) / \sim.$$

Per gli elementi di  $\mathbb{Q}$  usiamo la notazione standard sotto forma di frazione

$$\frac{a}{b} := \overline{(a, b)}, \quad \text{se } a, b \in \mathbb{Z} \text{ e } b \neq 0.$$

Notiamo che  $\boxed{\frac{a}{b} = \frac{a'}{b'}} \Leftrightarrow \overline{(a, b)} = \overline{(a', b')} \Leftrightarrow (a, b) \sim (a', b') \Leftrightarrow \boxed{ab' = a'b}.$

### Osservazione

*Se  $c \neq 0$ , poiché  $(ac)b = a(bc)$ , otteniamo la regola di riduzione  $\frac{ac}{bc} = \frac{a}{b}$ .*

Possiamo ora definire addizione e moltiplicazione in  $\mathbb{Q}$  ponendo per ogni  $\frac{m}{n}, \frac{p}{q} \in \mathbb{Q}$

$$\frac{m}{n} + \frac{p}{q} = \frac{mq+np}{nq} \quad (\text{somma}),$$

$$\frac{m}{n} \cdot \frac{p}{q} = \frac{mp}{nq} \quad (\text{prodotto}).$$

Anche in questo caso le operazioni sono definite tramite certi rappresentanti delle classi che definiscono  $\mathbb{Q}$  e quindi occorre verificare che siano ben definite.

## Proposizione

*L'addizione e la moltiplicazione sono ben definite.*

DIMOSTRAZIONE. Vogliamo che

$$+ : \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}, \left( \frac{m}{n}, \frac{p}{q} \right) \mapsto \frac{mq + np}{nq}$$

sia una funzione. Pertanto dobbiamo mostrare che

$$\left( \frac{m}{n}, \frac{p}{q} \right) = \left( \frac{m'}{n'}, \frac{p'}{q'} \right) \Rightarrow \frac{mq + np}{nq} = \frac{m'q' + n'p'}{n'q'}$$

L'uguaglianza di sinistra implica  $\frac{m}{n} = \frac{m'}{n'}$  e  $\frac{p}{q} = \frac{p'}{q'}$ , cioè  $mn' = m'n$  e  $pq' = p'q$ . Allora

$$(mq + np)n'q' = mn'qq' + nn'pq' = m'nqq' + nn'p'q = (m'q' + n'p')nq$$

da cui  $\frac{mq+np}{nq} = \frac{m'q'+n'p'}{n'q'}$ . Similmente  $mpn'q' = mn'pq' = m'np'q = m'p'nq$

da cui  $\frac{mp}{nq} = \frac{m'p'}{n'q'}$ . Pertanto anche la moltiplicazione è un'operazione.

## Proposizione (Immersione di $\mathbb{Z}$ in $\mathbb{Q}$ )

La funzione

$$\iota : \mathbb{Z} \rightarrow \mathbb{Q}, \quad z \mapsto \frac{z}{1},$$

è iniettiva e rispetta le operazioni di addizione e moltiplicazione, cioè, per ogni  $m, n \in \mathbb{Z}$ ,

$$\iota(m+n) = \iota(m) + \iota(n), \quad \iota(mn) = \iota(m) \cdot \iota(n).$$

Come per  $\mathbb{Z}$  si può dimostrare in  $\mathbb{Q}$  che

- l'addizione è associativa e commutativa, che
- $\frac{0}{1}$  è l'elemento neutro dell'addizione (cioè lo zero) e che
- $\frac{-m}{n}$  è un opposto di  $\frac{m}{n}$  (infatti  $\frac{-m}{n} + \frac{m}{n} = \frac{-mn+nm}{nn} = \frac{0}{nn} = \frac{0\cancel{nn}}{1\cancel{nn}} = \frac{0}{1}$ ).

L'opposto di  $\frac{m}{n}$  si indica, al solito, anche con il simbolo  $-\frac{m}{n}$ .

Inoltre per  $\mathbb{Q}$  si può dimostrare che la moltiplicazione è associativa, commutativa, che  $\frac{1}{1}$  è un elemento neutro e che  $\frac{m}{n}$  è invertibile solo se  $m \neq 0$  (l'inverso è  $\frac{n}{m}$ ).

# Costruzione dei numeri complessi

La costruzione di  $\mathbb{R}$  a partire da  $\mathbb{Q}$  necessita di tecniche più sofisticate di quelle base della teoria degli insiemi ed è tradizionalmente demandata ai corsi di Analisi.

Passiamo dunque direttamente alla costruzione di  $\mathbb{C}$  a partire da  $\mathbb{R}$ . L'obiettivo è di estendere  $\mathbb{R}$  e le sue operazioni ad un insieme più grande che permetta di estrarre radici quadrate senza restrizioni e quindi risolvere equazioni algebriche che non ammettono soluzione tra i numeri reali.

## Definizione

Si dice insieme dei **numeri complessi**, l'insieme

$$\mathbb{C} = \mathbb{R} \times \mathbb{R} = \{(a, b) \in \mathbb{R} \times \mathbb{R} \text{ tali che } a, b \in \mathbb{R}\}.$$

Definiamo ora l'addizione e la moltiplicazione, per ogni  $(r, s), (r', s') \in \mathbb{C}$ ,

$$(r, s) + (r', s') = (r + r', s + s') \quad (\text{somma componente per componente}),$$

$$(r, s) \cdot (r', s') = (rr' - ss', rs' + sr') \quad (\text{prodotto}).$$

## Osservazione

*Si vede subito che  $(\mathbb{C}, +) = (\mathbb{R}^2, +)$  è un monoide commutativo rispetto alla somma componente per componente e che lo zero (elemento neutro) è*

$$0_{\mathbb{C}} = (0_{\mathbb{R}}, 0_{\mathbb{R}}).$$

*Poiché  $(r, s) + (-r, -s) = (r - r, s - s) = (0_{\mathbb{R}}, 0_{\mathbb{R}})$  otteniamo che ogni elemento  $(r, s)$  ha un opposto  $(-r, -s)$ . Pertanto  $-(r, s) = (-r, -s)$ . Inoltre  $(\mathbb{C}, \cdot)$  risulta essere un monoide commutativo con elemento neutro*

$$1_{\mathbb{C}} = (1_{\mathbb{R}}, 0_{\mathbb{R}}).$$

*Vale inoltre la proprietà distributiva, cioè per ogni  $u, v, w \in \mathbb{C}$  si ha che*

$$(u + v) \cdot w = u \cdot w + v \cdot w.$$



## Lemma

*Un numero complesso è non nullo  $\Leftrightarrow$  è invertibile rispetto al prodotto. Più precisamente, se  $x, y \in \mathbb{R}$  sono tali che  $x \neq 0 \vee y \neq 0$ , allora*

$$(x, y)^{-1} = \left( \frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2} \right).$$

DIMOSTRAZIONE. Indichiamo con  $\mathbb{C}^\times$  l'insieme degli elementi invertibili in  $(\mathbb{C}, \cdot)$  e dimostriamo che  $\mathbb{C}^\times = \mathbb{C} \setminus \{0_{\mathbb{C}}\}$ .

( $\subseteq$ ). Preso  $z \in \mathbb{C}^\times$ , allora esiste il suo inverso  $z^{-1}$ . Se  $z$  fosse  $0_{\mathbb{C}}$ , allora si avrebbe  $0_{\mathbb{C}} \cdot z^{-1} = z \cdot z^{-1} = 1_{\mathbb{C}}$ . Ma dalla definizione di prodotto segue subito che moltiplicando per  $0_{\mathbb{C}}$  si ottiene sempre  $0_{\mathbb{C}}$ . Pertanto si avrebbe  $0_{\mathbb{C}} = 1_{\mathbb{C}}$ , cioè  $(0_{\mathbb{R}}, 0_{\mathbb{R}}) = (1_{\mathbb{R}}, 0_{\mathbb{R}})$ , da cui  $0_{\mathbb{R}} = 1_{\mathbb{R}}$ , assurdo. Pertanto  $z \neq 0_{\mathbb{C}}$  e dunque  $z \in \mathbb{C} \setminus \{0_{\mathbb{C}}\}$ .

( $\supseteq$ ). Sia  $z \in \mathbb{C} \setminus \{0_{\mathbb{C}}\}$ . Scritto  $z = (x, y) \in \mathbb{C} = \mathbb{R} \times \mathbb{R}$ , la condizione  $z \neq 0_{\mathbb{C}}$  significa  $(x, y) \neq (0, 0)$  cioè  $x \neq 0 \vee y \neq 0$ . In particolare si ha  $x^2 + y^2 \neq 0$ . Allora si vede subito, dalla definizione di prodotto che

$$(x, y) \cdot \left( \frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2} \right) = (1_{\mathbb{R}}, 0_{\mathbb{R}}) = 1_{\mathbb{C}}.$$

Controlliamo come  $\mathbb{C}$  sia un'estensione di  $\mathbb{R}$  con le sue operazioni.

### Proposizione (Immersione di $\mathbb{R}$ in $\mathbb{C}$ )

*La funzione  $\iota : \mathbb{R} \rightarrow \mathbb{C}, r \mapsto (r, 0_{\mathbb{R}})$ , è iniettiva e rispetta le operazioni di addizione e moltiplicazione.*

*Più precisamente, per ogni  $r, s \in \mathbb{R}$ , si ha che*

$$\iota(r+s) = \iota(r) + \iota(s), \quad \iota(0_{\mathbb{R}}) = 0_{\mathbb{C}}, \quad \iota(rs) = \iota(r) \cdot \iota(s), \quad \iota(1_{\mathbb{R}}) = 1_{\mathbb{C}}.$$

### Proof.

E' iniettiva perché  $\iota(a) = \iota(b)$  vuol dire  $(a, 0_{\mathbb{R}}) = (b, 0_{\mathbb{R}})$  e quindi  $a = b$ .

Inoltre

$$\begin{aligned} \iota(r) + \iota(s) &= (r, 0_{\mathbb{R}}) + (s, 0_{\mathbb{R}}) = (r+s, 0_{\mathbb{R}} + 0_{\mathbb{R}}) = (r+s, 0_{\mathbb{R}}) = \iota(r+s), \\ \iota(0_{\mathbb{R}}) &= (0_{\mathbb{R}}, 0_{\mathbb{R}}) = 0_{\mathbb{C}}, \\ \iota(r) \cdot \iota(s) &= (r, 0_{\mathbb{R}}) \cdot (s, 0_{\mathbb{R}}) = (r \cdot s - 0_{\mathbb{R}} \cdot 0_{\mathbb{R}}, r \cdot 0_{\mathbb{R}} + 0_{\mathbb{R}} \cdot s) = (rs, 0_{\mathbb{R}}) = \iota(rs), \\ \iota(1_{\mathbb{R}}) &= (1_{\mathbb{R}}, 0_{\mathbb{R}}) = 1_{\mathbb{C}}, \end{aligned}$$

per ogni  $r, s \in \mathbb{R}$ , come segue subito dalle definizioni delle operazioni.  $\square$

## Lemma (Legge di annullamento del prodotto)

$\forall w, z \in \mathbb{C}$  si ha che  $w \cdot z = 0_{\mathbb{C}} \Rightarrow w = 0_{\mathbb{C}} \vee z = 0_{\mathbb{C}}$ .

DIMOSTRAZIONE. Abbiamo visto che, se  $w \neq 0_{\mathbb{C}}$ , allora  $w$  è invertibile rispetto al prodotto. Pertanto  $w \cdot z = 0_{\mathbb{C}} \Rightarrow w^{-1} \cdot w \cdot z = w^{-1} \cdot 0_{\mathbb{C}}$ . Il prodotto per  $0_{\mathbb{C}}$  fa sempre zero e quindi otteniamo  $1_{\mathbb{C}} \cdot z = 0_{\mathbb{C}}$  cioè  $z = 0_{\mathbb{C}}$ .

---

Definiamo **unità immaginaria** il numero complesso

$$i = (0_{\mathbb{R}}, 1_{\mathbb{R}}).$$

Notiamo che, per ogni  $a, b \in \mathbb{R}$ ,

$$\iota(a) + \iota(b) \cdot i = (a, 0_{\mathbb{R}}) + (b, 0_{\mathbb{R}}) \cdot (0_{\mathbb{R}}, 1_{\mathbb{R}}) = (a, 0_{\mathbb{R}}) + (0_{\mathbb{R}}, b) = (a, b).$$

Quindi  $(a, b) = \iota(a) + \iota(b) \cdot i$ . Per snellire la notazione, al posto di  $\iota(a)$  si scriverà semplicemente “ $a$ ”, e quindi  $(a, b) = a + b \cdot i$ .

Inoltre il segno di moltiplicazione si omette scrivendo  $(a, b) = a + bi$ .