NUMERI INTERI

Generalità

È noto che, mentre l'equazione $x - 5 = 0$ è risolubile in $\mathbb{N}$, l'equazione $x + 3 = 0$ non lo è, pertanto dobbiamo cercare di *ampliare l'insieme dei numeri* in modo da includere tutte le soluzioni di equazioni del tipo $x + n = 0, n \in \mathbb{N}$.

Giungiamo quindi all'insieme $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3\}$, detto insieme degli **interi relativi**. Per dare la definizione degli interi relativi, partiamo dal prodotto cartesiano $\mathbb{N} \times \mathbb{N}$, ovvero l'insieme delle coppie ordinate di numeri naturali, e introduciamo questa relazione:

$$\boxed{(n, m) \ \sim \ (n', m') \iff n + m' = m + n'}$$

Esempio - Rappresentazione di un numero intero

$(5, 6) \sim (0, 1) \iff 5 + 1 = 6 + 0$
$(8, 2) \sim (6, 0) \iff 8 + 0 = 2 + 6$

Dimostriamo che questa relazione sia di equivalenza:

- È **riflessiva**: $(a, b)\ \rho\ (a, b) \iff a + b = a + b$
- È **simmetrica**: $(a, b)\ \rho\ (c, d) \implies (c, d)\ \rho\ (a, b) : c + b = a + d$, e $a + d = c + b$ per ipotesi
- È **transitiva**: $(a, b)\ \rho\ (c, d)$ e $(c, d)\ \rho\ (e, f) \implies (a, b)\ \rho\ (e, f)$:

$$\begin{cases} a + d = b + c \\ c + f = d + e, \end{cases} \overset{\text{sommando}}{\implies} a + d + c + f = b + c + d + e \implies (a, b)\ \rho\ (e, f)$$

  Si tratta di una *relazione di equivalenza.* L'insieme $\mathbb{N} \times \mathbb{N}$ viene quindi diviso in classi (n, m).

Possiamo quindi definire delle classi di equivalenza che suddividono in parti l'insieme $\mathbb{N}\times\mathbb{N}$ in classi $[(n, m)]$. Scegliamo come *rappresentanti* delle classi di equivalenza gli elementi che prevedono **uno dei due elementi uguale a** 0.

Ogni classe sarà rappresentabile con uno dei seguenti rappresentanti distinti:

$$\begin{gathered} (0, 0) \\ (1, 0), (2, 0), (3, 0) \dots, (n, 0) \dots \\ (0, 1), (0, 2), (0, 3) \dots, (0, n) \dots \end{gathered}$$

In sintesi, una coppia del tipo $(a,0)$ è *in relazione con tutte le coppie* $(n,m)|n-m=a$:

$$*_1 : [7,0] = \{(10,3)(14,7),(15,8),\dots\}$$

mentre una coppia del tipo $(0,a)$ è *in relazione con tutte le coppie* $(n,m)|n-m=-a$:

$$*_2 : [0,2] = \{(4,6),(8,10),(9,11),\dots\}$$

Pertanto, l'insieme quoziente $\mathbb{Z} := \mathbb{N}\times\mathbb{N}/\sim$ è detto **insieme dei numeri interi**.

Possiamo quindi definire

$$\begin{aligned}\mathbb{Z}^+ &\overset{\text{def}}{=} \{\overline{(n,0)}|n\in\mathbb{N}, n\neq 0\}\\ 0 &\overset{\text{def}}{=} \overline{(0,0)}\\ \mathbb{Z}^- &\overset{\text{def}}{=} \{\overline{(0,n)}|n\in\mathbb{N}, n\neq 0\}\end{aligned}$$

Mentre gli elementi di $\mathbb{Z}$ nel seguente modo:

$$\begin{aligned}\overline{(n,0)} &\overset{\text{def}}{=} n\\ \overline{(0,0)} &\overset{\text{def}}{=} 0\\ \overline{(0,n)} &\overset{\text{def}}{=} -n\end{aligned}$$

I numeri interi godono delle proprietà base:

- Proprietà **commutativa** dell'addizione
- Proprietà *associativa* dell'addizione
- Esistenza dell'***elemento neutro*** rispetto all'addizione
- Esistenza dell'opposto
- Proprietà **commutativa** della moltiplicazione
- Proprietà *associativa* della moltiplicazione
- Esistenza dell'***elemento neutro*** rispetto alla moltiplicazione
- **Distributiva** della moltiplicazione rispetto all'addizione

LEMMA: Siano a, b elementi di $\mathbb{Z}$. Allora:

- $a*0=0*a=0$
- $(-a)*b=-(a*b)$
- $(-a)(-b)=ab$

Valore Assoluto

Si definisce *valore assoluto* di un intero a il numero intero positivo

$$|a| = \begin{cases} a & \text{se } a \geq 0 \\ -a & \text{se } a < 0 \end{cases}$$

Dati quindi $a, b \in \mathbb{Z}$ valgono le seguenti relazioni

$$|a| + |b| \geq |a + b| \quad \text{e} \quad |a| * |b| = |a * b|$$

Divisibilità

DEF: dati due interi a, b si dice che a *divide* b e si scrive $a|b$, se esiste un $c \in \mathbb{Z}$ tale che $b = ac$.

DEF: in un anello commutativo si dice che un elemento $a \neq 0$ è un *divisore dello zero* se esiste un $b \neq 0$ tale che $ab = 0$.

DEF: un *dominio di integrità* è un anello commutativo primo di divisori dello 0.

DEF: è un divisore comune degli elementi a e b di $\mathbb{Z}$ un elemento $c \in \mathbb{Z}$ tale che $c|a$ e $c|b$.

Lemma: Se c'è un *divisore comune* di a e b, allora c divide ogni intero della forma $sa + tb$, con s e t in $\mathbb{Z}$ cioè $c|a$ e $c|b \implies c|sa + tb \, \forall s, t \in \mathbb{Z}$.

DEF: Un elemento $u \in \mathbb{Z}$ che divide 1 si dice una *unità* (elemento invertibile) di $\mathbb{z}$.
E' immediato riconoscere che le sole unità di $\mathbb{Z}$ sono 1 e -1

DEF: due elementi a e b di $\mathbb{Z}$ tali che $a|b$ e $b|a$ si dicono associati
Possiamo quindi dire che due elementi sono associati se e solo se differiscono per il segno. La relazione associati è una relazione di equivalenza.

DEF: un elemento $a \in \mathbb{Z}$ che non sia lo zero e non sia una unità si dice *primo* se ogni volta che a divide un prodotto bc, con $b, c \in \mathbb{Z}$, allora a divide almeno uno dei due fattori.

PROPOSIZIONE: ogni elemento primo in $\mathbb{Z}$ è un elemento irriducibile.

- **DIMOSTRAZIONE:** sia a un elemento primo in $\mathbb{Z}$. Per provare che esso è irriconducibile dobbiamo provare che dall''essere $a = bc$ con $b, c \in \mathbb{Z}$ segue che b o c sono delle unità. Sia dunque $a = bc$; in particolare $a|bc$.
  Allora (essendo a primo per ipotesi) $a|b$ oppure $a|c$, cioè $b = ah$ o $c = ak$ con $h, k \in \mathbb{Z}$; ma allora la $a = bc$, assieme ad una di queste relazioni comportano che a o b o c sono delle unità