ALGEBRA I: ASSIOMI DI PEANO E PROPRIETÀ DEI NUMERI NATURALI

1. Gli assiomi di Peano

Come puro esercizio di stile voglio offrire una derivazione delle proprietà elementari dei numeri naturali e delle operazioni definite su $\mathbb{N}$. L'unica struttura originaria di $\mathbb{N}$ è il principio di induzione, pertanto la definizione di tutti i concetti primitivi come la relazione d'ordine e le operazioni di somma e prodotto è fatta per ricorrenza, e le loro proprietà sono dimostrate per induzione. Man mano che i concetti sono definiti e le proprietà dimostrate, le tecniche diventano più mature, e le dimostrazioni più naturali. I concetti primitivi necessari per definire l'insieme $\mathbb{N}$ dei numeri naturali sono un elemento $0 \in \mathbb{N}$, anche detto *zero*, ed un'applicazione iniettiva $s : \mathbb{N} \to \mathbb{N}$, detta *successivo*, che non ha 0 nella sua immagine. Gli assiomi di Peano sono in effetti

- $0 \in \mathbb{N}$;
- $s : \mathbb{N} \to \mathbb{N}$ è iniettiva e $0 \notin s(\mathbb{N})$;
- Vale il *principio di induzione*: **se $X \subset \mathbb{N}$ è un sottoinsieme che contiene 0 e tale che $s(X) \subset X$, allora $X = \mathbb{N}$.**

In generale, per mostrare che un sottoinsieme $X \subset \mathbb{N}$ coincide con $\mathbb{N}$ si mostra prima che $0 \in X$ e poi che $n \in X \Rightarrow s(n) \in X$ per ogni $n \in \mathbb{N}$. Allo stesso modo, per definire una proprietà o un'operazione su ogni elemento di $\mathbb{N}$ è sufficiente farlo per lo 0 e per $s(n)$ ogni volta che la definizione sia già stata data per n: la definizione è data, in altri termini, *ricorsivamente* o *per ricorrenza*.

Per mostrare che un enunciato $p(n), n \in \mathbb{N}$ è vero per ogni n è sufficiente mostrare che vale $p(0)$ (*base dell'induzione*) e che dalla validità di $p(n)$ (*ipotesi induttiva*) segue (*passo induttivo*) quella di $p(s(n))$ per ogni n. L'enunciato viene dimostrato così *per induzione*.

Lemma 1.1. *Se $a \in \mathbb{N}$ è diverso da 0, allora $a = s(a')$ per qualche $a' \in \mathbb{N}$.*

Dimostrazione. Se $p(a)$ indica l'implicazione

$$a \neq 0 \Rightarrow \exists a' \in \mathbb{N} \text{ tale che } a = s(a'),$$

dobbiamo mostrare che $p(a)$ è vera per ogni $a \in \mathbb{N}$. Lo facciamo per induzione su a.

La base dell'induzione $p(0)$ è banalmente vera in quanto l'ipotesi è falsa. Per mostrare il passo induttivo dobbiamo far vedere che se $p(n)$ è vera, allora lo è anche $p(s(n))$. Ma in effetti $p(s(n))$ è vera a prescindere da $p(n)$, perché $s(n)$ si ottiene applicando s all'elemento n. □

2. Il buon ordinamento di $\mathbb{N}$

Siamo pronti a definire la relazione d'ordine $\leq$ su $\mathbb{N}$. Ricordo che una relazione è nota una volta che siano noti gli elementi che mette in relazione.

Definizione 2.1. La relazione $\leq$ è definita ricorsivamente come segue:

- $0 \leq b$ per ogni scelta di $b \in \mathbb{N}$;
- $s(a) \leq b$ se e solo se $b = s(b')$ con $a \leq b'$.

Lemma 2.2. *Valgono le seguenti proprietà:*

(1) *$s(a)$ non è mai ≤ 0;*
(2) *Se $a \leq 0$ allora $a = 0$;*
(3) *$a \leq b$ se e solo se $s(a) \leq s(b)$.*

Dimostrazione. Gli assiomi di Peano garantiscono che $s(a) \neq 0$. Ma per definizione, affinché $s(a) \leq b$ è necessario che b sia della forma $s(b')$, e quindi diverso da 0, il che mostra (1). (2) segue allora facilmente: supponiamo per assurdo che $a \neq 0$. Allora $a = s(a')$ per qualche $a' \in \mathbb{N}$, e la definizione di $\leq$ mostra che $s(a') \leq 0$ non è possibile. L'ultima affermazione è una semplice riformulazione dalla definizione di $\leq$. □

Corollario 2.3. *Non si ha mai $s(0) \leq 0$. Allo stesso modo $s(m)$ non è mai $\leq m$.*

Corollario 2.4. *Se $a \leq s(0)$, allora $a = 0$ oppure $a = s(0)$.*

Dimostrazione. Se $a \neq 0$, allora $a = s(a')$ per qualche a'. Ma allora da $s(a') \leq s(0)$ segue $a' \leq 0$ e quindi $a' = 0$. □

Proposizione 2.5. *La relazione $\leq$ definisce su $\mathbb{N}$ un ordinamento totale.*

Dimostrazione. Bisogna mostrare che $\leq$ è una relazione d'ordine, cioè che soddisfa le proprietà riflessiva, antisimmetrica e transitiva; e inoltre che comunque scelti $a, b \in \mathbb{N}$ almeno una tra $a \leq b$ e $b \leq a$ è vera.

- **Riflessività**. Sia $0 \leq 0$ che $n \leq n \Rightarrow s(n) \leq s(n)$ seguono dalla definizione di $\leq$. Ma allora $a \leq a$ è vera per ogni $a \in \mathbb{N}$ per induzione su a.

- **Antisimmetria**. Dobbiamo mostrare che $a \leq b, b \leq a \Rightarrow a = b$ per ogni scelta di $a, b \in \mathbb{N}$, e lo facciamo per induzione su a. La base dell'induzione $a = 0$ segue dal Lemma 2.2 che mostra come da $b \leq 0$ si ottenga $b = 0$. Per quanto riguarda il passo induttivo, supponiamo che $s(n) \leq b, b \leq s(n)$. Da $s(n) \leq b$ segue $b = s(b')$ per qualche $b' \in \mathbb{N}$. Ma $s(n) \leq s(b'), s(b') \leq s(n)$ valgono se e solo se valgono $n \leq b', b' \leq n$. Per ipotesi induttiva abbiamo allora $n = b'$ e quindi $s(n) = s(b') = b$.
- **Transitività**. Mostro per induzione su a che $a \leq b, b \leq c \Rightarrow a \leq c$. La base dell'induzione $a = 0$ segue immediatamente, in quanto $0 \leq c$ è sempre vera. Per quanto riguarda il passo induttivo, da $s(a) \leq b$ segue $b = s(b')$, e da $b = s(b') \leq c$ segue $c = s(c')$. Ma allora $s(a) \leq s(b'), s(b') \leq s(c')$ e di conseguenza $a \leq b', b' \leq c'$ da cui $a \leq c'$ per ipotesi induttiva. Pertanto $s(a) \leq s(c') = c$.
- **Ordinamento totale**. Mostriamo per induzione su a che, comunque presi $a, b \in \mathbb{N}$, vale $a \leq b$ oppure $b \leq a$. La base dell'induzione $a = 0$ è chiara, in quanto $0 \leq b$ è comunque vera. Il passo induttivo richiede di mostrare che, comunque scelti $a, b \in \mathbb{N}$, si ha $s(a) \leq b$ oppure $b \leq s(a)$. Questo è chiaro se $b = 0$, in quanto $0 \leq s(a)$. Se invece $b \neq 0$, allora $b = s(b')$, e dobbiamo solamente stabilire che almeno una tra $a \leq b'$ e $b' \leq a$ è vera, che è garantito dall'ipotesi induttiva.

□

E' comune scrivere $a < b$ se $a \leq b$ ma $a \neq b$. Chiaramente, $a \not\leq b$ se e solo se $b < a$, in quanto $\leq$ è un ordinamento totale. Inoltre $a < b$ se e solo se $s(a) < s(b)$.

Lemma 2.6. *Se $a \leq b < s(a)$ allora $a = b$*

Dimostrazione. Per induzione su a. La base dell'induzione $a = 0$ è chiara: infatti se $b < s(0)$ con $b \neq 0$ si ha $b = s(b')$, ma allora $s(b') < s(0)$ è equivalente a $b' < 0$, che è impossibile. Dimostriamo ora il passo induttivo: se $s(a) \leq b < s(s(a))$, dalla prima disuguaglianza si ricava $b = s(b')$. Ma allora $s(a) \leq s(b') < s(s(a))$ è equivalente a $a \leq b' < s(a)$, da cui $a = b'$ per ipotesi induttiva, e quindi $s(a) = s(b') = b$. □

Abbiamo ora tutti gli strumenti per dimostrare che $\leq$ è un buon ordinamento.

Teorema 2.7. *Ogni sottoinsieme non vuoto di $\mathbb{N}$ possiede un elemento minimo rispetto all'ordinamento $\leq$.*

Dimostrazione. Sia X un sottoinsieme di $\mathbb{N}$ privo di elemento minimo. Voglio mostrare che l'insieme

$$Y = \{n \in \mathbb{N} \,|\, m \in X \Rightarrow m \geq s(n)\}$$

coincide con tutto $\mathbb{N}$. In effetti 0 appartiene a Y altrimenti, per la definizione dell'insieme Y, 0 apparterrebbe ad X, e ne sarebbe l'elemento minimo, contrariamente alle ipotesi fatte.

Se accadesse che $n \in Y$ ma $s(n) \notin Y$, allora esisterebbe $m \in X$ tale che $m \geq s(n)$ ma $m \not\geq s(s(n))$. Quindi $s(n) \leq m < s(s(n))$ e $m = s(n)$ appartiene ad X. Ma da $n \in Y$ segue che gli elementi di X sono tutti $\geq s(n)$ e quindi $s(n)$ è minimo in X, un assurdo. Pertanto se $n \in Y$ allora anche $s(n) \in Y$. Possiamo concludere che Y coincide con $\mathbb{N}$, e quindi che se $m \in X$, allora $m \geq s(n)$ per ogni $n \in \mathbb{N}$. Ma $m \geq s(m)$ è impossibile, quindi X è vuoto.

Abbiamo dimostrato che ogni sottoinsieme di $\mathbb{N}$ privo di elemento minimo è vuoto, o equivalentemente che ogni sottoinsieme non vuoto di $\mathbb{N}$ possiede un elemento minimo. □

3. L'operazione di somma

Lavorare con $\mathbb{N}$ utilizzando soltanto l'operazione primitiva di successivo può essere scomodo, laborioso e frustrante. E' quindi opportuno definire immediatamente il concetto di somma di elementi di $\mathbb{N}$.

Definizione 3.1. L'applicazione $\mathbb{N} \times \mathbb{N} \ni (a, b) \mapsto a + b \in \mathbb{N}$ è definita (ricorsivamente in a) da:

- $0 + b = b$;
- $s(a) + b = s(a + b)$.

L'elemento $a + b$ si dice *somma* degli elementi a e b.

Lemma 3.2. *$s(0) + b = s(b)$ per ogni $b \in \mathbb{N}$.*

Dimostrazione. Dalla definizione dell'operazione di somma segue che $s(0) + b = s(0 + b) = s(b)$. □

Generalmente, $s(0)$ viene indicato con 1. Abbiamo quindi appena visto che $s(n) = 1 + n$ per ogni $n \in \mathbb{N}$. L'operazione di successivo si ottiene dalla somma aggiungendo 1 (a sinistra, perché non sappiamo ancora che la somma è commutativa) all'argomento.

Proposizione 3.3. *La somma è un'operazione associativa, cioè $(a + b) + c = a + (b + c)$ per ogni scelta di $a, b, c \in \mathbb{N}$.*

Dimostrazione. Per induzione su a. La base dell'induzione è chiara: in effetti $(0 + b) + c = b + c = 0 + (b + c)$. Anche la dimostrazione del passo induttivo è semplice: $(s(a) + b) + c = s(a + b) + c = s((a + b) + c)$, mentre $s(a) + (b + c) = s(a + (b + c))$; comunque $(a + b) + c = a + (b + c)$ per ipotesi induttiva, e quindi

$$(s(a) + b) + c = s((a + b) + c) = s(a + (b + c)) = s(a) + (b + c).$$

□

Lemma 3.4. *$a + 0 = a$ per ogni $a \in \mathbb{N}$.*

Dimostrazione. Per induzione su a. $0 + 0 = 0$ è chiaro. Inoltre se $a + 0 = a$, allora $s(a) + 0 = s(a + 0) = s(a)$. □

Lemma 3.5. *$a + 1 = 1 + a$ per ogni $a \in \mathbb{N}$.*

Dimostrazione. Alla luce del Lemma 3.2, dobbiamo mostrare che $a + s(0) = s(a)$ per ogni $a \in \mathbb{N}$: lo facciamo per induzione su a.

La base dell'induzione è chiara, in quanto $0 + s(0) = s(0)$. Il passo induttivo segue facilmente: $s(a) + s(0) = s(a + s(0))$, e sappiamo per ipotesi induttiva che $a + s(0) = s(a)$. Quindi $s(a) + s(0) = s(a + s(0)) = s(s(a))$. □

Possiamo finalmente concludere che $s(n) = n + 1 = 1 + n$ per ogni $n \in \mathbb{N}$.

Proposizione 3.6. *L'operazione di somma è commutativa, cioè $a + b = b + a$ per ogni scelta di $a, b \in \mathbb{N}$.*

Dimostrazione. Per induzione su a. La base dell'induzione segue dalla definizione e dal Lemma 3.4. Il passo induttivo si dimostra utilizzando ripetutamente l'associatività della somma (Proposizione 3.3), il Lemma 3.5 e l'ipotesi induttiva:

$$s(a) + b = (a + 1) + b = a + (1 + b) = a + (b + 1) = (a + b) + 1 = (b + a) + 1 = b + (a + 1) = b + s(a).$$

□

Molto utile è la proprietà di cancellazione della somma.

Proposizione 3.7. *Siano $a, b, c \in \mathbb{N}$. Allora $a + c = b + c$ se e solo se $a = b$.*

Dimostrazione. Per induzione su c, la base dell'induzione essendo ovvia. Per quanto riguarda il passo induttivo, da $a + (c + 1) = b + (c + 1)$ segue per associatività $(a + c) + 1 = (b + c) + 1$ cioè $s(a + c) = s(b + c)$. Ma s è iniettiva, quindi $a + c = b + c$, e possiamo ora utilizzare l'ipotesi induttiva. □

E' importante sottolineare che nella manipolazione degli elementi di $\mathbb{N}$ eviteremo rigorosamente di rappresentarli attraverso l'applicazione ripetuta di s a 0. Non scriveremo mai $s^3(0)$ o $s(s(s(0)))$, ma più semplicemente 3. In generale $s(s(\dots(0)\dots)) = s^n(0)$ sarà rappresentato dall'esponente n. Poiché la somma di $s^m(0)$ e $s^n(0)$ risulta essere $s^{m+n}(0)$, la nostra notazione per la somma coincide con quella usuale.

Riassumendo, abbiamo finora mostrato che è possibile definire su $\mathbb{N}$ un'operazione di somma associativa e commutativa, della quale 0 è l'elemento neutro, che permette di rappresentare l'operazione s di prendere il successivo per mezzo di $s(n) = n + 1$. Vale inoltre l'utile proprietà di cancellazione descritta nella Proposizione 3.7.

4. Somma, ordine e differenza

Sia l'operazione di somma che la relazione d'ordine sono state definite a partire dal concetto primitivo di successivo descritto dall'applicazione s. Non è quindi sorprendente che la somma e l'ordinamento siano compatibili in vari modi. Il lemma che segue traduce l'idea intuitiva che sommando ad un elemento di $\mathbb{N}$ un altro elemento se ne ottiene uno più grande.

Lemma 4.1. *$a \leq a + b$ per ogni scelta di $a, b \in \mathbb{N}$.*

Dimostrazione. Per induzione su a, la base $0 \leq b$ dell'induzione essendo chiaramente vera. Il passo induttivo è immediato, poiché $a \leq a + b$ se e solo se $s(a) \leq s(a + b)$ da cui $s(a) \leq s(a) + b$. □

Più interessante è l'affermazione che segue:

Lemma 4.2. *Se a e c sono elementi di $\mathbb{N}$ tali che $a \leq c$, allora esiste b in $\mathbb{N}$ tale che $c = a + b$.*

Dimostrazione. Ancora una volta per induzione su a. Se $a = 0$ non c'è nulla da dimostrare, perché $c = 0 + c$. Per il passo induttivo, se $a + 1 = s(a) \leq c$, allora $c = s(c')$ per qualche c', e $a \leq c'$. Ma allora $c' = a + b$, da cui $c = c' + 1 = (a + 1) + b$. □

L'elemento b si chiama differenza di c ed a, e si indica con $c - a$. Si noti che è univocamente determinato da a e da c, in quanto se $a + b_1 = a + b_2$, allora per la Proposizione 3.7 si ha $b_1 = b_2$. Abbiamo quindi dimostrato la seguente

Proposizione 4.3. *$a \leq b$ se e solo se esiste un elemento che sommato ad a fornisce b come risultato. Tale elemento è unico, una volta scelti a e b, e si indica con $b - a$.*

Chiaramente, $a - a = 0$ e $(a + b) - a = b$. La Proposizione 4.3 spiega che "*il meno si può fare solo quando il primo numero è più grande*".

Lemma 4.4. *Se $a, b, c \in \mathbb{N}$, allora $a \leq b$ è vera esattamente quando è vera $a + c \leq b + c$.*

Dimostrazione. Per induzione su c, la base dell'induzione essendo ovvia. Il passo induttivo è anche ovvio, dal momento che $a + (c + 1) = (a + c) + 1$ e $b + (c + 1) = (b + c) + 1$. Quindi $a + (c + 1) \leq b + (c + 1)$ se e solo se $s(a + c) \leq s(b + c)$ se e solo se $a + c \leq b + c$. □

Lemma 4.5. *Se $a \leq c$ e $b \leq d$ allora $a + b \leq c + d$.*

Dimostrazione. Per il Lemma 4.4, $a + b \leq c + b$ e $b + c \leq c + d$. La tesi segue ora dalla transitività di $\leq$ e dalla commutatività della somma. □

5. L'operazione di moltiplicazione

La seconda importante operazione da definire sull'insieme $\mathbb{N}$ dei numeri naturali è la *moltiplicazione*.

Definizione 5.1. L'operazione $\mathbb{N} \times \mathbb{N} \ni (a, b) \mapsto a \cdot b \in \mathbb{N}$ è definita (ricorsivamente in a) da:

- $0 \cdot b = 0$;
- $(a + 1) \cdot b = a \cdot b + b$.

L'elemento $a \cdot b$ si dice *prodotto* degli elementi a e b.

Osservazione 5.2. E' evidente dalla definizione che $1 \cdot b = b$ in quanto $(0 + 1) \cdot b = 0 \cdot b + b = 0 + b = b$. Pertanto si ha $(a + 1) \cdot b = a \cdot b + 1 \cdot b$, che è una prima elementare forma di distributività del prodotto rispetto alla somma, vera più in generale.

Proposizione 5.3. *Per ogni scelta di $a, b, c \in \mathbb{N}$, si ha $(a + b) \cdot c = a \cdot c + b \cdot c$.*

Dimostrazione. Per induzione su a, il caso $a = 0$ essendo immediato. Per l'osservazione appena fatta, abbiamo $((a + 1) + b) \cdot c = ((a + b) + 1) \cdot c = (a + b) \cdot c + c$. Usando allora l'ipotesi induttiva, insieme con l'associatività e la commutatività della somma, si ottiene

$$((a + 1) + b) \cdot c = (a + b) \cdot c + c = (a \cdot c + b \cdot c) + c = (a \cdot c + c) + b \cdot c = (a + 1) \cdot c + b \cdot c.$$

□

La distributività destra è un po' più delicata di quella sinistra.

Lemma 5.4. *$a \cdot 0 = 0$ per ogni $a \in \mathbb{N}$.*

Dimostrazione. E' chiaro se $a = 0$. Allo stesso modo $(a + 1) \cdot 0 = a \cdot 0 + 1 \cdot 0 = 0$. L'enunciato è quindi dimostrato per induzione. □

Lemma 5.5. *$a \cdot 1 = a$ per ogni $a \in \mathbb{N}$.*

Dimostrazione. E' chiaro se $a = 0$. Inoltre $(a + 1) \cdot 1 = a \cdot 1 + 1$ e la tesi segue per ipotesi induttiva. □

Lemma 5.6. *$a \cdot (b + 1) = a \cdot b + a$ per ogni $a, b \in \mathbb{N}$.*

Dimostrazione. Per induzione su a. La base $a = 0$ dell'induzione è chiara. Per il passo induttivo

$$(a + 1) \cdot (b + 1) = a \cdot (b + 1) + (b + 1) = (a \cdot b + a) + (b + 1) = (a \cdot b + b) + (a + 1) = (a + 1) \cdot b + (a + 1).$$

□

Proposizione 5.7. *Per ogni scelta di $a, b, c \in \mathbb{N}$, si ha $a \cdot (b + c) = a \cdot b + a \cdot c$.*

Dimostrazione. Per induzione su b, il caso $b = 0$ essendo ovvio. Per quanto riguarda il passo induttivo, abbiamo:

$$a \cdot ((b + 1) + c) = a \cdot (b + (c + 1)) = a \cdot b + a \cdot (c + 1) = a \cdot b + a \cdot c + a = (a \cdot b + a) + a \cdot c = a \cdot (b + 1) + a \cdot c.$$

□

Proposizione 5.8. *La moltiplicazione è commutativa, cioè $a \cdot b = b \cdot a$ per ogni $a, b \in \mathbb{N}$.*

Dimostrazione. Per induzione su a. Il caso $a = 0$ è chiaro, perché entrambi i membri sono uguali a zero. Dimostriamo allora il passo induttivo. Si ha $(a + 1) \cdot b = a \cdot b + b$, e $b \cdot (a + 1) = b \cdot a + b$. Per ipotesi induttiva, sappiamo già che $a \cdot b = b \cdot a$, e quindi $(a + 1) \cdot b = a \cdot b + b = b \cdot a + b = b \cdot (a + 1)$. □

Come ci si aspetta, la moltiplicazione è anche associativa.

Proposizione 5.9. *Per ogni scelta di $a, b, c \in \mathbb{N}$ si ha $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.*

Dimostrazione. Per induzione su a. Quando $a = 0$, entrambi i prodotti sono nulli, e l'affermazione è quindi vera. Dimostriamo allora il passo induttivo. Abbiamo:

$$((a + 1) \cdot b) \cdot c = (a \cdot b + b) \cdot c = (a \cdot b) \cdot c + b \cdot c,$$

mentre

$$(a + 1) \cdot (b \cdot c) = a \cdot (b \cdot c) + b \cdot c.$$

Sappiamo per ipotesi induttiva che $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, e quindi coincidono anche le quantità appena calcolate. □

6. Prodotto, ordine e cancellazione

Studiando la compatibilità della relazione d'ordine con la moltiplicazione possiamo ricavare le principali proprietà di cancellazione di tale operazione.

Lemma 6.1. *Se $b \neq 0$, allora $a \leq a \cdot b$ per ogni $a \in \mathbb{N}$.*

Dimostrazione. Per induzione su a. Se $a = 0$ la tesi diventa $0 \leq 0$, che è chiaramente vera. Altrimenti, da $a \leq a \cdot b$ e $1 \leq b$ segue $a + 1 \leq a \cdot b + b = (a + 1) \cdot b$. □

La legge di annullamento del prodotto è ora di dimostrazione immediata.

Proposizione 6.2. *Se $a \cdot b = 0$ e $b \neq 0$, allora $a = 0$.*

Dimostrazione. Per il lemma precedente, abbiamo $a \leq a \cdot b = 0$, da cui $a = 0$. □

Avendo dimostrato che in un prodotto nullo almeno uno dei fattori è nullo, la proprietà di cancellazione del prodotto è anch'essa immediata.

Proposizione 6.3. *Se $a \neq 0$ e $a \cdot b = a \cdot c$, allora $b = c$.*

Dimostrazione. $\leq$ è una relazione d'ordine totale, quindi a meno di scambiare b e c possiamo supporre che $b \leq c$. Allora, per la Proposizione 4.3, esiste $h \in \mathbb{N}$ tale che $c = b + h$, da cui $a \cdot c = a \cdot b + a \cdot h$.

Sappiamo che $a \cdot b = a \cdot c$, quindi per la proprietà di cancellazione della somma concludiamo che $a \cdot h = 0$. La Proposizione 6.2 garantisce ora che $h = 0$ e quindi che $c = b + h = b$. □

Lemma 6.4. *Se $b \leq c$, allora $a \cdot b \leq a \cdot c$.*

Dimostrazione. Dal momento che $b \leq c$, la Proposizione 4.3 ci assicura che esiste $h \in \mathbb{N}$ tale che $c = b + h$. Ma allora $a \cdot c = a \cdot b + a \cdot h$ e quindi $a \cdot b \leq a \cdot c$. □

In particolare, se $b \leq c$ si ha $a \cdot c - a \cdot b = a \cdot (c - b)$. L'enunciato del lemma appena dimostrato si rovescia quando $a \neq 0$.

Lemma 6.5. *Se $a \neq 0$ e $a \cdot b \leq a \cdot c$ allora $b \leq c$.*

Dimostrazione. Per assurdo. Se $c < b$ allora $b = c + h$ con $h \neq 0$. Ma allora $a \cdot b = a \cdot c + a \cdot h$, con $a \cdot h \neq 0$ per la Proposizione 6.2. Quindi $a \cdot c < a \cdot b$, che è assurdo. □

Lemma 6.6. *Se $a \leq c$ e $b \leq d$, allora $a \cdot b \leq c \cdot d$.*

Dimostrazione. Da $a \leq c$ segue $a \cdot b \leq c \cdot b$, mentre da $b \leq d$ segue $b \cdot c \leq d \cdot c$. Utilizzando la transitività di $\leq$ e la commutatività del prodotto, si ottiene $a \cdot b \leq b \cdot c \leq c \cdot d$. □

Abbiamo già verificato che 1 è tale che $1 \cdot a = a \cdot 1 = a$ per ogni $a \in \mathbb{N}$. Questo fatto si esprime dicendo che 1 è l'*elemento neutro* della moltiplicazione. Un naturale a si dice *invertibile* se si può trovare un naturale b tale che $a \cdot b = 1$. Gli elementi invertibili sono importanti nello studio delle proprietà di fattorizzazione, ma tra i numeri naturali 1 è l'unico elemento invertibile.

Proposizione 6.7. *Se $a \cdot b = 1$, allora $a = b = 1$.*

Dimostrazione. Il Lemma 6.1 ci assicura che $a \leq a \cdot b$. Quindi $a \leq 1$, e per il Corollario 2.4 gli unici valori possibili per a sono 0 e 1. Comunque se $a = 0$, allora $a \cdot b = 0$, quindi a deve essere uguale ad 1. Lo stesso ragionamento può essere ripetuto per b. □

Se non mi sbaglio, ho dimostrato tutte le proprietà algebriche dell'insieme $\mathbb{N}$ dei numeri naturali elencati nel libro di Campanella. Sono le proprietà intuitive che usiamo senza timori nelle ordinarie manipolazioni di questi numeri. Il mio scopo era quello di mostrare come fosse possibile ricavarle dagli assiomi di Peano, e come quindi tali assiomi catturino gli aspetti fondamentali delle proprietà dei numeri naturali.

Dipartimento di Matematica, Università degli studi di Roma – "La Sapienza"
E-mail address: dandrea@mat.uniroma1.it