Insiemi finiti e sommatorie

Pino Vigna Suria

4 novembre 2007

1 Insiemi finiti

Per ogni numero naturale n poniamo $\overline{n} = \{p \in \mathbb{N} \text{ tali che } 1 \leq p \leq n\}$. In particolare $\overline{0} = \emptyset$.

Definizione 1. *Un insieme A si dice* finito *se esistono un numero naturale n ed una biezione $f : \overline{n} \longrightarrow A$.*

L'insieme vuoto è finito perché la funzione vuota $\overline{0} \longrightarrow \emptyset$ è biettiva.

Lemma 1. *Siano $n, m \in \mathbb{N}$. $n \leq m$ se e solo se esiste una funzione iniettiva $\overline{n} \longrightarrow \overline{m}$.*

Dimostrazione. Se $n \leq m$ l'inclusione $\overline{n} \hookrightarrow \overline{m}$ è iniettiva.

Viceversa, sia $U = \{n \in \mathbb{N} \text{ tali che }, \forall m \in \mathbb{N}, \text{ se esiste una funzione iniettiva } \overline{n} \longrightarrow \overline{m} \text{ allora } n \leq m\}$. Proviamo che $U = \mathbb{N}$. Certamente $0 \in U$. Supponiamo che $n \in U$ e proviamo che $n + 1 \in U$. Sia dunque $m \in \mathbb{N}$ e $f : \overline{n+1} \longrightarrow \overline{m}$ una funzione iniettiva. Dobbiamo provare che $n + 1 \leq m$. Certamente $m \neq 0$ perché non esistono funzioni (e dunque nemmeno funzioni iniettive) $\emptyset \neq \overline{n+1} \longrightarrow \emptyset = \overline{0}$. Quindi esiste $p \in \mathbb{N}$ tale che $m = p + 1$. Poniamo $a = f(n + 1)$ e sia $h : \overline{m} \longrightarrow \overline{m}$ la biezione che scambia tra loro a con m e fissa tutti gli altri elementi. Allora $h \circ f : \overline{n+1} \longrightarrow \overline{m}$ è ancora iniettiva (in quanto composizione di due funzioni iniettive) e manda $n + 1$ in $m = p + 1$, perciò la sua restrizione a $\overline{n}$ è una funzione iniettiva $\overline{n} \longrightarrow \overline{p}$. Siccome $n \in U$ avremo che $n \leq p$ e quindi $n + 1 \leq p + 1 = m$. □

Se A è un insieme finito, m, n sono numeri naturali e $f : \overline{n} \longrightarrow A$, $g : \overline{m} \longrightarrow A$ sono biettive allora $g^{-1} \circ f : \overline{n} \longrightarrow \overline{m}$ e $f^{-1} \circ g : \overline{m} \longrightarrow \overline{n}$ sono

iniettive , e dunque, per il lemma 1, $n \leq m$ e $m \leq n$, cioè $n = m$. Tale numero è detto *il numero di elementi di* A e indicato con $\sharp A$, in particolare $\sharp\emptyset = 0$.

Il lemma 1 si generalizza nella

Proposizione 1. *Siano* A, B *insiemi finiti.* $\sharp A \leq \sharp B$ *se e solo se esiste una funzione iniettiva* $A \longrightarrow B$.

Dimostrazione. Siano $\sharp A = n$, $\sharp B = m$, $f : \overline{n} \longrightarrow A$ e $g : \overline{m} \longrightarrow B$ biezioni.

Se $n \leq m$, per il lemma 1 esiste una funzione iniettiva $g : \overline{n} \longrightarrow \overline{m}$. Ma allora $g \circ h \circ f^{-1} : A \longrightarrow B$ è iniettiva.

Viceversa se $h : A \longrightarrow B$ è iniettiva, $g^{-1} \circ h \circ f : \overline{n} \longrightarrow \overline{m}$ è iniettiva e per il solito lemma $n \leq m$. □

Proposizione 2. *Sia* A *un insieme finito, e* B *un insieme. Le seguenti affermazioni sono equivalenti*

1. B *è finito e* $\sharp B = \sharp A$.

2. *Esiste una corrispondenza biunivoca tra* A *e* B:

Dimostrazione. $1 \Rightarrow 2$ Supponiamo che $\sharp A = \sharp B = n$ e siano $f : \overline{n} \longrightarrow A$ e $g : \overline{n} \longrightarrow B$ delle biezioni. Allora $g \circ f^{-1} : A \longrightarrow B$ è una biezione.

$2 \Rightarrow 1$ Supponiamo che $\sharp A = n$ e siano $f : \overline{n} \longrightarrow A$ e $g : A \longrightarrow B$ delle biezioni. Allora $g \circ f : \overline{n} \longrightarrow B$ è una biezione. □

Proposizione 3. *Ogni sottoinsieme di un insieme finito è finito, anzi se* $\sharp A = n$ *e* $B \subseteq A$ *allora* $\sharp B \leq \sharp A$. *Se* $\sharp B = \sharp A$ *allora* $B = A$.

Dimostrazione. Sia $M = \{p \in \mathbb{N}$ tali che esiste una funzione iniettiva $\overline{p} \longrightarrow B\}$. Certamente $M \neq \emptyset$ perché la funzione vuota $\overline{0} = \emptyset \longrightarrow B$ è iniettiva e dunque $0 \in M$.

Affermo che, per ogni $p \in M$, $p \leq n$. Infatti, se esiste $h : \overline{p} \longrightarrow B$ ed esiste $f : \overline{n} \longrightarrow A$ biettiva, allora la restrizione a B di f^{-1} è una funzione iniettiva $B \longrightarrow \overline{n}$ e dunque la sua composizione con h è una funzione iniettiva $\overline{p} \longrightarrow \overline{n}$, e, per il lemma 1, $p \leq n$. Quindi l'insieme non vuoto M è superiormente limitato (da n) e dunque ha un massimo minore o uguale a n, chiamiamolo q. Questo significa che $q \in M$, e dunque esiste una funzione iniettiva $g : \overline{q} \longrightarrow B$, ma $q+1 \notin M$. Affermo che g è biettiva, il che conclude la dimostrazione. Infatti se, per assurdo esiste $b \in B$ tale che $b \notin \mathrm{Im}g$, allora possiamo definire

$h : \overline{q+1} \longrightarrow B$ ponendo $h(t) = g(t)$ se $t \in \overline{q}$ e $h(q+1) = b$. Questa funzione è ancora iniettiva, contraddicendo il fatto che $q + 1 \notin M$.

Per quanto riguarda l'ultima affermazione, supponiamo, per assurdo, che $a \in A - B$ e che $g : \overline{n} \longrightarrow B$ sia biettiva. Definiamo $h : \overline{n+1} \longrightarrow B$ ponendo $h(t) = g(t)$ se $t \in \overline{n}$ e $h(n+1) = a$. Si tratta ancora di una funzione iniettiva e allora $f^{-1} \circ h : \overline{n+1} \longrightarrow \overline{n}$ sarebbe ancora iniettiva, contraddicendo il lemma 1. □

Proposizione 4. *L'unione di due insiemi finiti e disgiunti A, B è finita, e*

$$\sharp A \cup B = \sharp A + \sharp B$$

Dimostrazione. Siano $\sharp A = n$, $\sharp B = m$, $f : \overline{n} \longrightarrow A$ e $g : \overline{m} \longrightarrow B$ biezioni. Definiamo $h : \overline{n+m} \longrightarrow A \cup B$ mediante

$$h(t) = \begin{cases} f(t) & \text{se} \quad t \leq n \\ g(t-n) & \text{se} \quad t > n \end{cases}$$

Notiamo che, se $n < t \leq n+m$ allora $t - n \in \overline{m}$ e quindi ha senso applicargli la g. Si verifica facilmente che h è una biezione, l'unico punto non facilissimo è che se $t \leq n$ e $s > n$ allora $h(t) \neq h(s)$; ma $h(t) = f(t) \in A$, mentre $h(s) = g(s-n) \in B$ e $A \cap B = \emptyset$. □

Proposizione 5. *L'unione di due insiemi finiti è finita e*

$$\sharp A \cup B = \sharp A + \sharp B - \sharp A \cap B$$

Dimostrazione. Notiamo che $A \cap B$ è finito in quanto sottoinsieme di A (si veda la proposizione 3). Poniamo $C = B - (A \cap B)$, allora C e $A \cap B$ sono disgiunti e quindi, per la proposizione 4, $\sharp B = \sharp C \cup (A \cap B) = \sharp C + \sharp A \cap B$. Ma anche $A \cap C = \emptyset$ e, usando la stessa proposizione si ha che $\sharp A + \sharp C = \sharp A \cup C = \sharp A \cup B$. Con un po' di aritmetica infantile si conclude. □

Proposizione 6. *Il prodotto cartesiano di due insiemi finiti è finito e*

$$\sharp A \times B = \sharp A \cdot \sharp B$$

Dimostrazione. Cominciamo trovando esplicitamente, per ogni $n, m \in \mathbb{N}$ una corrispondenza biunivoca tra gli insiemi $\overline{n} \times \overline{m}$ e $\overline{nm}$. Se $n = 0$ o $m = 0$ la funzione vuota assolve lo scopo. Supponiamo perciò che i numeri siano entrambi non nulli, e quindi anche $nm \neq 0$.

La funzione σ che ad ogni numero naturale p associa il suo successore $p+1$ stabilisce evidentemente una corrispondenza biunivoca tra $\{0,\dots,n-1\}$ e $\overline{n}$ e anche tra $\{0,\dots,m-1\}$ e $\overline{m}$ e tra $\{0,\dots,nm-1\}$ e $\overline{nm}$. Definiamo una funzione

$$\phi : \{0,\dots,n-1\} \times \{0,\dots,m-1\} \longrightarrow \{0,\dots,nm-1\}$$

mediante $\phi(p,q) = mp+q$. Certamente, per ogni $(p,q) \in \{0,\dots,n-1\} \times \{0,\dots,m-1\}$ avremo che $0 = 0m+0 \leq pm+q \leq (n-1)m+m-1 = nm-1$, e quindi la funzione effettivamente agisce tra i due insiemi proposti. Per provare che è biettiva ragioniamo così: l'algoritmo di divisione ci assicura che, per ogni $r \in \mathbb{N}$, esistono e sono unici $t \in \mathbb{N}$ e $s \in \{0,\dots,m-1\}$ tali che $r = tm+s$. Ci basta allora verificare che, se $r \in \{0,\dots,nm-1\}$, allora $t \in \{0,\dots,n-1\}$, e difatti, se fosse $t \geq n$ allora $r = tm+s \geq tm \geq nm > nm-1$.

Quindi la funzione $\psi : \overline{n} \times \overline{m} \longrightarrow \overline{nm}$ data da

$$\psi(x,y) = (x-1)m + (y-1) + 1 = (x-1)m + y$$

è una biezione.

Adesso passiamo al caso generale: siano $\sharp A = n$, $\sharp B = m$, $f : \overline{n} \longrightarrow A$ e $g : \overline{m} \longrightarrow B$ biezioni. La funzione $f \times g : \overline{n} \times \overline{m} \longrightarrow A \times B$ che manda (p,q) in $(f(p), g(q))$ è una biezione e allora $(f \times g) \circ \psi^{-1}$ è una biezione tra $\overline{nm}$ e $A \times B$. □

Definiamo un'operazione binaria interna su $\mathbb{N}$ mandando la coppia ordinata (n,m) in n^m definito ricorsivamente così: se $m \in \mathbb{N}$, $m^0 = 1$ e $m^{n+1} = m^n \cdot m$.

Se A, B sono insiemi, denotiamo con B^A l'insieme di tutte le funzioni $A \longrightarrow B$. Se $A = \emptyset$ allora, per ogni insieme B, B^A ha un elemento, la funzione vuota.

Proposizione 7. *Se A, B sono insiemi finiti anche B^A è finito e*

$$\sharp B^A = \sharp B^{\sharp A}$$

Dimostrazione. Sia

$$U = \{n \in \mathbb{N} \text{ tali che } \forall A \text{ tale che } \sharp A = n,$$

$$\forall m \in \mathbb{N}, \forall B \text{ tale che } \sharp B = m,\ \sharp B^A = m^n\}$$

e cerchiamo di provare per induzione che $U = \mathbb{N}$.

Le osservazioni sulla definizione dell'esponenziale di insiemi e numeri ci garantiscono che $0 \in U$. Supponiamo che $n \in U$ e proviamo che allora anche $n+1 \in U$. Sia A un insieme con $n+1$ elementi, $m \in \mathbb{N}$ e B un insieme con m elementi. Scegliamo $a \in A$, poniamo $A' = A - \{a\}$. Grazie alla proposizione 4, avremo che $\sharp A' = n$ e quindi, dato che $n \in U$, $\sharp B^{A'} = m^n$: Definiamo una funzione $\psi : B^A \longrightarrow B^{A'} \times B$ ponendo $\psi(f) = (f_{|A'}, f(a))$. Si vede facilmente che ψ è una biezione e quindi, usando la proposizione 2 e la proposizione 6, si ha che

$$\sharp B^A = \sharp B^{A'} \cdot \sharp B = m^n \cdot m = m^{n+1}$$

Quindi $n + 1 \in U$ e la dimostrazione è conclusa. □

Corollario 1. *Se A è un insieme finito anche il suo insieme delle parti $\mathcal{P}(A)$ lo è e*

$$\sharp(\mathcal{P}(A)) = 2^{\sharp A}$$

Dimostrazione. Definiamo una funzione $\psi : \overline{2}^A \longrightarrow \mathcal{P}(A)$ mediante $\psi(f) = \{a \in A \text{ tali che } f(a) = 2\}$. Si vede facilmente che ψ è una biezione e quindi, usando la proposizione 2 e la proposizione 7, si ha la tesi. □

Per ogni numero naturale n ricordiamo che il *fattoriale* di n è il numero naturale $n!$ definito per ricorsività come segue: $0! = 1,\ (n+1)! = n! \cdot (n+1)$.

Se A è un insieme, indichiamo con S_A l'insieme di tutte le biezioni in A^A; equipaggiando questo insieme con l'operazione di composizione si ha un gruppo (non commutativo se A ha più di due elementi) che si chiama il *gruppo delle permutazioni* di A. Se $A = \overline{n}$ si scrive S_n in sostituzione di $\mathrm{S}_{\overline{n}}$.

Proposizione 8. *Se A è un insieme finito anche S_A è finito e $\sharp \mathrm{S}_A = \sharp A!$.*

Dimostrazione. Dimostriamo dapprima il risultato nel caso $A = \overline{n}$. Sia $U = \{n \in \mathbb{N} \text{ tali che } \sharp \mathrm{S}_n = n!\}$. $0 \in U$ perché $\mathrm{S}_0 = \mathrm{S}_\emptyset$ ha un solo elemento, la funzione vuota.

Supponiamo ora che $n \in U$ e dimostriamo che $n + 1 \in U$. Poniamo $\mathrm{S}'_{n+1} = \{\sigma \in \mathrm{S}_{n+1} \text{ tali che } \sigma(n + 1) = n + 1\}$. Evidentemente la funzione $\mathrm{S}'_{n+1} \longrightarrow \mathrm{S}_n$ che associa ad ogni elemento di S'_{n+1} la sua restrizione a $\overline{n}$ è una biezione e, visto che $n \in U$, usando la proposizione 2 abbiamo che $\sharp \mathrm{S}'_{n+1} = n!$.

Per ogni $a \in \overline{n+1}$ chiamiamo h^a l'elemento di S_{n+1} che scambia a con $n + 1$ e fissa tutti gli altri elementi di $\overline{n+1}$. Naturalmente $h^{n+1} = \mathrm{id}_{\overline{n+1}}$ e, per ogni $a \in \overline{n+1}$, $\quad h^a \circ h^a = \mathrm{id}_{\overline{n+1}}$.

Definiamo ora una funzione

$$\psi : \mathrm{S}_{n+1} \longrightarrow \mathrm{S}'_{n+1} \times \overline{n+1}$$

mediante $\psi(\sigma) = (h^{\sigma(n+1)} \circ \sigma, \sigma(n+1))$; cioè: dato σ, calcoliamo $a = \sigma(n+1)$, poi poniamo $\sigma' = h^a \circ \sigma$, che effettivamente sta in S'_{n+1} in quanto $\sigma'(n+1) = h^a(\sigma(n+1)) = h^a(a) = n+1$. Così abbiamo che $\psi(\sigma) = (\sigma', a) = (h^a \circ \sigma, a)$.

Definiamo poi una funzione

$$\phi : \mathrm{S}'_{n+1} \times \overline{n+1} \longrightarrow \mathrm{S}_{n+1}$$

mediante $\phi(\sigma', a) = h^a \circ \sigma'$.

Verifichiamo che ψ e ϕ sono funzioni inverse l'una dell'altra, e quindi sono biezioni. $\forall (\sigma', a) \in \mathrm{S}'_{n+1} \times \overline{n+1}$

$$\psi \circ \phi(\sigma', a) = \psi(h^a \circ \sigma') = (h^a \circ (h^a \circ \sigma'), a) = ((h^a \circ h^a) \circ \sigma'), a) = (\sigma', a)$$

$\forall \sigma \in \mathrm{S}_{n+1}$ poniamo $a = \sigma(n+1)$ e così

$$\phi \circ \psi(\sigma) = \phi(h^a \circ \sigma, a) = h^a \circ (h^a \circ \sigma) = (h^a \circ h^a) \circ \sigma = \sigma$$

Dalle proposizioni 2 e 6 segue che $\sharp \mathrm{S}_{n+1} = \sharp \mathrm{S}'_{n+1} \cdot \sharp \overline{n+1} = n! \cdot (n+1) = (n+1)!$.

Nel caso generale, se $\sharp A = n$ e $f : \overline{n} \longrightarrow A$ è una biezione, si assegna una corrispondenza biunivoca tra S_n e S_A mandando σ in $f \circ \sigma \circ f^{-1}$. Di nuovo si conclude con l'aiuto della proposizione 2. □

La lettrice attenta avrà osservato, in queste note, una sgradevole invadenza delle funzioni iniettive a scapito di quelle suriettive. Ad esempio il lemma 1 dice, in soldoni, che non si può andare dal grande al piccolo in modo iniettivo, cioè senza ripetizioni. La nostra intuizione ci dice che non si può andare dal piccolo al grande in modo suriettivo, cioè coprendo tutto il codominio, il che, in termini rigorosi, ci istiga a proporre la

Proposizione 9. *Siano $n, m \in \mathbb{N}$. $n \geq m$ se e solo se esiste una funzione suriettiva $\overline{n} \longrightarrow \overline{m}$.*

Disgraziatamente questo non è vero, infatti $5 \geq 0$ ma non esistono funzioni suriettive $\overline{5} \longrightarrow \overline{0} = \emptyset$, in quanto non esistono funzioni tout court tra questi insiemi. Tuttavia l'unica eccezione è proprio questa patologia e quindi possiamo correggere la congettura così:

Proposizione 10. *Siano $n, m \in \mathbb{N}$.*

1. *Se esiste una funzione suriettiva $\overline{n} \longrightarrow \overline{m}$ allora $n \geq m$.*
2. *Se $n \geq m \neq 0$ allora esiste una funzione suriettiva $\overline{n} \longrightarrow \overline{m}$.*

Dimostrazione. $1 \Rightarrow 2$. Se $n = 0$, l'unica funzione $\overline{n} \longrightarrow \overline{m}$ è la funzione vuota; essa deve essere suriettiva e allora $m = 0$ e quindi $n \geq m$.

Supponiamo ora $n \neq 0$ e che esista una funzione suriettiva $f : \overline{n} \longrightarrow \overline{m}$. L'esistenza di tale funzione (non importa che sia suriettiva) impone $m \neq 0$. Inoltre, per ogni $y \in \overline{m}$, l'insieme $f^{-1}(y) = \{x \in \overline{n} \text{ tali che } f(x) = y\}$ non è vuoto. Definiamo $g : \overline{m} \longrightarrow \overline{n}$ mediante $g(y) = \min f^{-1}(y)$. Così otterremo che $f \circ g = \mathrm{id}_{\overline{m}}$, ed, in particolare, g è iniettiva. Per il lemma 1 abbiamo proprio che $m \leq n$, la tesi.

$2 \Rightarrow 1$. La funzione $f : \overline{n} \longrightarrow \overline{m}$ definita da

$$f(x) = \begin{cases} x & \text{se} \quad x \leq m \\ 1 & \text{se} \quad x > m \end{cases}$$

è palesemente suriettiva. □

Scimmiottando la dimostrazione della proposizione 1 si vede facilmente che l'ultima proposizione si generalizza facilmente nella

Proposizione 11. *Siano A, B insiemi finiti.*

1. *Se esiste una funzione suriettiva $A \longrightarrow B$ allora $\sharp A \geq \sharp B$.*
2. *Se $B \neq \emptyset$ e $\sharp A \geq \sharp B$ allora esiste una funzione suriettiva $A \longrightarrow B$.*

Proposizione 12. *Siano A, B insiemi finiti tali che $\sharp A = \sharp B$. Una funzione $f : A \longrightarrow B$ è iniettiva se e solo se è suriettiva.*

Dimostrazione. L'affermazione è palesemente vera se $A = B = \emptyset$. Escludiamo questo caso. Supponiamo che f sia iniettiva, ma, per assurdo, non suriettiva, cioè $\mathrm{Im} f \subsetneq B$. Allora le funzione $f : A \longrightarrow \mathrm{Im} f$ è ancora iniettiva. Ma, per la proposizione 3, $\sharp \mathrm{Im} f < \sharp B = \sharp A$ e questo contraddice la proposizione 1.

Viceversa supponiamo che f sia suriettiva ma, per assurdo non iniettiva. Allora esistono $x \neq y \in A$ tali che $f(x) = f(y)$ e sia $A' = A - \{x\}$. Allora, sempre per la proposizione 3, $\sharp A' < \sharp A = \sharp B$ e la funzione $f_{|A'} : A' \longrightarrow B$ è ancora suriettiva. Questo contraddice la proposizione 11. □

2 Sommatorie

Cominciamo con il definire la somma di $n-$uple ordinate.

Se X è un insieme, si ricorda che, nonostante le molte definizioni o più spesso non-definizioni che si possono trovare in letteratura, una $n-$upla ordinata in X è semplicemente una funzione $\overline{n} \longrightarrow X$, la $0-$upla ordinata è la funzione vuota; l'insieme di tutte le $n-$uple ordinate in X viene indicato con X^n in luogo del classico $X^{\overline{n}}$. Se $\alpha : \overline{m} \longrightarrow \overline{n}$ è una funzione e $v \in X^n$ allora $v \circ \alpha$ è una $m-$upla ordinata in X. In particolare, se $m \leq n$ la restrizione a $\overline{m}$ di v è una $m-$upla ordinata.

Sia $(V, +)$ un semigruppo abeliano, cioè V è un insieme, $+$ è un'operazione binaria interna associativa e commutativa su V, con elemento neutro 0. Indichiamo con $\bigcup_{n\in\mathbb{N}} V^n$ l'insieme di tutte le n-uple ordinate di V, al variare di n tra i numeri naturali.

Possiamo definire per ricorsività una funzione $\phi : \bigcup_{n\in\mathbb{N}} V^n \longrightarrow V$ caratterizzata dalle seguenti condizioni

- Se $v \in V^0$, cioè v è la funzione vuota, allora $\phi(v) = 0$
- Per ogni $n \in \mathbb{N}$ e per ogni $v \in V^{n+1}$, $\phi(v) = \phi(v_{|\overline{n}}) + v_{n+1}$

Notiamo che, per ogni $v \in V^1$, $\phi(v) = v_1$. In seguito, quando non saremo più condizionati da superstizioni ataviche, useremo una notazione molto più accattivante per la funzione ϕ; la lettrice che si senta corazzata alle lusinghe di una terminologia troppo rivelatrice può azzardarsi a guardare subito alla notazione 1 a pagina 10. A suo rischio.

Per ogni numero naturale n e per ogni $k \leq n$ definiamo $\alpha_n^k : \overline{k} \longrightarrow \overline{n}$ mediante $\alpha_k^n(i) = n - k + i$ (in particolare α_n^0 è la funzione vuota e α_n^n è l'identità). Conviene anche dare il nome $\rho_n^k : \overline{k} \longrightarrow \overline{n}$ alla funzione di inclusione; evidentemente, se $p \leq k \leq n$ abbiamo che

$$\rho_n^k \circ \rho_k^p = \rho_n^p, \quad \alpha_n^k \circ \alpha_k^p = \alpha_n^p \quad \text{e} \quad \rho_n^k \circ \alpha_k^p = \alpha_n^{n-k+p} \circ \rho_{n-k+p}^p \tag{1}$$

La seconda condizione che definisce la funzione ϕ si scrive

Per ogni $n \in \mathbb{N}$ e per ogni $v \in V^{n+1}$

$$\phi(v) = \phi(v \circ \rho_{n+1}^n) + \phi(v \circ \alpha_{n+1}^1) \tag{2}$$

Lemma 2. *Per ogni $n \geq 1$ e per ogni $v \in V^n$*

$$\phi(v) = v_1 + \phi(v \circ \alpha_n^{n-1}) = \phi(v \circ \rho_n^1) + \phi(v \circ \alpha_n^{n-1})$$

Dimostrazione. Per induzione su n. Se $n = 1$ e $v \in V^1$, $\phi(v) = v_1 = v_1 + 0 = v_1 + \phi(v \circ \alpha_1^0)$ in quanto $v \circ \alpha_1^0$ è la funzione vuota.

Per ogni $n \geq 2$ e per ogni $v \in V^{n+1}$ abbiamo che

$$\phi(v) = \phi(v \circ \rho_{n+1}^n) + \phi(v \circ \alpha_{n+1}^1) = (v_1 + \phi(v \circ \rho_{n+1}^n \circ \alpha_n^{n-1})) + \phi(v \circ \alpha_{n+1}^1) =$$

$$v_1 + (\phi(v \circ \alpha_{n+1}^n \circ \rho_n^{n-1}) + \phi(v \circ \alpha_{n+1}^n \circ \alpha_n^1)) = v_1 + \phi(v \circ \alpha_{n+1}^n)$$

che è quanto si desiderava. Si noti l'uso della proprietà associativa. □

Per generalizzare questo risultato abbiamo bisogno della

Proposizione 13 (Principio di induzione retrograda)**.** *Siano* $1 \leq n \in \mathbb{N}$ *e* $U \subseteq \overline{n}$ *tale che*

- $n \in U$
- *Per ogni* $k \in \overline{n}$*, se* $k + 1 \in U$ *allora* $k \in U$*.*

Allora $U = \overline{n}$*.*

Dimostrazione. Supponiamo, per assurdo, che $\overline{n} - U$ non sia vuoto. Trattandosi di un insieme limitato avrà un massimo, $k < n$ per la prima condizione. Ma allora $k + 1 \in U$ mentre $k \notin U$, contraddicendo la seconda. □

Proposizione 14. *Per ogni* $k \leq n \in \mathbb{N}$ *e per ogni* $v \in V^n$*,*

$$\phi(v) = \phi(v \circ \rho_n^k) + \phi(v \circ \alpha_n^{n-k})$$

Dimostrazione. Sia U l'insieme dei k che soddisfano la proprietà. $n \in U$ banalmente in quanto ρ_n^n è l'identità e α_n^0 è la funzione vuota.

Supponiamo che $k + 1 \in U$ e sia $v \in V^n$. Sappiamo che

$$\phi(v) = \phi(v \circ \rho_n^{k+1}) + \phi(v \circ \alpha_n^{n-k-1})$$

Applichiamo l'equazione 2 alla $(k+1)-$upla $v \circ \rho_n^{k+1}$ e otteniamo

$$\phi(v) = (\phi(v \circ \rho_n^{k+1} \circ \rho_{k+1}^k) + \phi(v \circ \rho_n^{k+1} \circ \alpha_{k+1}^1)) + \phi(v \circ \alpha_n^{n-k-1})$$

Usando la proprietà associativa e l'equazione 1 abbiamo

$$\phi(v) = \phi(v \circ \rho_n^k) + (\phi(v \circ \alpha_n^{n-k} \circ \rho_{n-k}^1) + \phi(v \circ \alpha_n^{n-k} \circ \alpha_{n-k}^{n-k-1}))$$

Infine applicando il lemma 2 alla $(n-k)-$upla $v \circ \alpha_n^{n-k}$ otteniamo

$$\phi(v) = \phi(v \circ \rho_n^k) + \phi(v \circ \alpha_n^{n-k})$$

cioè $k \in U$ e la dimostrazione è conclusa. □

Finalmente, sicuri di non esercene fatti influenzare a causa della sua assenza, introduciamo la notazione tradizionale.

Notazione 1. *Per ogni $k \leq n \in \mathbb{N}$ e per ogni $v \in V^n$ definiamo*

- $\displaystyle\sum_{i=1}^{n} v_i = \phi(v)$
- $\displaystyle\sum_{i=1}^{k} v_i = \phi(v \circ \rho_n^k)$
- $\displaystyle\sum_{i=n-k+1}^{n} v_i = \phi(v \circ \alpha_n^k)$

Così abbiamo che $\sum_{i=1}^{0} v_i = 0$, $\sum_{i=n+1}^{n} v_i = 0$, rifrasando la proposizione 14, si ha $\sum_{i=1}^{k} v_i + \sum_{i=k+1}^{n} v_i = \sum_{i=1}^{n} v_i$ e, applicandola alla $(n-k)-$upla $v \circ \alpha_n^{n-k}$ abbiamo che, per ogni $k \leq r \leq n$ vale l'onnicomprensiva

$$\sum_{i=k+1}^{r} v_i + \sum_{i=r+1}^{n} v_i = \sum_{i=k+1}^{n} v_i \tag{3}$$

Notiamo che non abbiamo mai usato la proprietà commutativa. Ma adesso lo facciamo.

Proposizione 15. *Per ogni $n \in \mathbb{N}$, $v \in V^n$, $\sigma \in \mathrm{S}_n$,*

$$\phi(v \circ \sigma) = \phi(v), \ \textit{cioè} \ \sum_{i=1}^{n} v_i = \sum_{i=1}^{n} v_{\sigma(i)}$$

Dimostrazione. Per induzione su n, sia U l'insieme dei numeri naturali per cui vale la proposizione. Evidentemente $0 \in U$; supponiamo che $n \in U$ e siano $v \in V^{n+1}$ e $\sigma \in \mathrm{S}_{n+1}$. Useremo pesantemente la terminologia introdotta nelle dimostrazione della proposizione 8.

Esaminiamo prima due casi speciali. Supponiamo che $\sigma(n+1) = n+1$, cioè $\sigma \circ \rho_{n+1}^n \in \mathrm{S}_n$, allora

$$\sum_{1}^{n+1} v_{\sigma(i)} = \sum_{1}^{n} v_{\sigma(i)} + v_{\sigma(n+1)} = \sum_{1}^{n} v_i + v_{n+1} = \sum_{1}^{n+1} v_i$$

Adesso supponiamo che σ scambi $n+1$ con un elemento $a \in \overline{n}$ e lasci fermi gli altri elementi di $\overline{n+1}$ (cioè σ è uno degli h^a menzionati nella dimostrazione della proposizione 8). Allora

$$\sum_1^{n+1} v_{\sigma(i)} = \sum_1^{a} v_{\sigma(i)} + \sum_{i=a+1}^{n+1} v_{\sigma(i)} = (\sum_1^{a-1} v_i + v_{\sigma(a)}) + (\sum_{i=a+1}^{n} v_{\sigma(i)} + v_{\sigma(n+1)}) =$$

$$(\sum_1^{a-1} v_{\sigma(i)} + v_{n+1}) + (\sum_{i=a+1}^{n} v_{\sigma(i)} + v_a) = (\sum_1^{a-1} v_{\sigma(i)} + v_{n+1}) + (v_a + \sum_{i=a+1}^{n} v_{\sigma(i)}) =$$

$$((\sum_1^{a-1} v_i + v_{n+1}) + v_a) + \sum_{i=a+1}^{n} v_i = (\sum_1^{a-1} v_i + (v_{n+1} + v_a)) + \sum_{i=a+1}^{n} v_i =$$

$$(\sum_1^{a-1} v_i + (v_a + v_{n+1})) + \sum_{i=a+1}^{n} v_i = ((\sum_1^{a-1} v_i + v_a) + v_{n+1}) + \sum_{i=a+1}^{n} v_i =$$

$$(\sum_1^{a-1} v_i + v_a) + (v_{n+1} + \sum_{i=a+1}^{n} v_i) = \sum_1^{a} v_i + (\sum_{i=a+1}^{n} v_i + v_{n+1}) =$$

$$\sum_1^{a} v_i + \sum_{i=a+1}^{n+1} v_i = \sum_{i=1}^{n+1} v_i$$

Noioso ma facile. Il caso generale segue facilmente, infatti ogni $\sigma \in \mathrm{S}_{n+1}$ può essere scritto come $h^a \circ \tau$, dove τ fissa $n+1$ e allora $\phi(v \circ \sigma) = \phi(v \circ h^a \circ \tau) = \phi(v \circ h^a) = \phi(v)$. Quindi $n+1 \in U$ e la dimostrazione è conclusa. □

Se X è un insieme indichiamo con $\mathrm{Fin}(X)$ l'insieme di tutti i sottoinsiemi finiti di X.

Teorema 1. *Esiste un'unica funzione*

$$\begin{array}{ccc} \mathrm{Fin}(X) \times V^X & \xrightarrow{\Sigma} & V \\ (A, f) & \mapsto & \sum_{a \in A} f(a) \end{array}$$

caratterizzata da

- $\sum_{a \in \emptyset} f(a) = 0$

- $\forall A \in \mathrm{Fin}(X),\ A \neq \emptyset,\ \forall a \in A,\ \sum_{b\in A} f(b) = \sum_{b\in A-\{a\}} f(b) + f(a)$

In particolare, per ogni $a \in X,\ \sum_{b\in\{a\}} f(b) = f(a)$.

Dimostrazione. Cominciamo a provare l'unicità. Siano

$$\Gamma,\ \Sigma : \mathrm{Fin}(X) \times V^X \longrightarrow V$$

due funzioni che soddisfano quanto richiesto, e sia

$$U = \{n \in \mathbb{N} \text{ tali che } \forall A \in \mathrm{Fin}(X) \text{ tale che } \sharp A = n,\ \forall f \in V^X,\ \Gamma(A,f) = \Sigma(A,f)\}$$

Certamente $0 \in U$ in quanto, per ogni $f \in V^X,\ \Gamma(\emptyset, f) = 0 = \Sigma(\emptyset, f)$.

Supponiamo che $n \in U$ e sia $A \in \mathrm{Fin}(X)$ tale che $\sharp A = n+1$ e sia $a \in A$, allora $\sharp(A - \{a\}) = n$ e, per ogni $f \in V^X$

$$\Gamma(A,f) = \Gamma(A-\{a\},f) + f(a) = \Sigma(A-\{a\},f) + f(a) = \Sigma(A,f)$$

quindi anche $n+1 \in U$ e l'unicità è provata.

Per quanto riguarda l'esistenza, se $A \in \mathrm{Fin}(X)$ esiste un unico numero naturale n ed una corrispondenza biunivoca $\alpha : \overline{n} \longrightarrow A$. Per ogni $f \in V^X,\ f \circ \alpha \in V^n$ e allora poniamo $\Sigma(A,f) = \sum_{a\in A} f(a) = \phi(f \circ \alpha)$. Controlliamo che questa definizione non dipende dalla scelta di α. Infatti se $\beta : \overline{n} \longrightarrow A$ è un'altra corrispondenza biunivoca, allora $\sigma = \beta^{-1} \circ \alpha \in \mathrm{S}_n$ e quindi, grazie alla proposizione 15, $\phi(f \circ \alpha) = \phi(f \circ \beta \circ \sigma) = \phi(f \circ \beta)$.

Dobbiamo controllare che Σ soddisfa le proprietà richieste. Se $A = \emptyset$ allora $f \circ \alpha \in V^0$ e quindi $\phi(f \circ \alpha) = 0$. Se $\sharp A = n+1$ e $a \in A$, sia $\alpha : \overline{n} \longrightarrow A - \{a\}$ una corrispondenza biunivoca. Definiamo una corrispondenza biunivoca $\alpha' : \overline{n+1} \longrightarrow A$ mediante $\alpha'_{|\overline{n}} = \alpha$ e $\alpha'(n+1) = a$, così avremo che

$$\Sigma(A,f) = \phi(f \circ \alpha') = \phi(f \circ \alpha) + (f \circ \alpha')_{n+1} = \Sigma(A-\{a\},f) + f(a)$$

e la dimostrazione è conclusa. □

Prendendo $(V,+) = (\mathbb{N},+)$ e indicando con $1 \in \mathbb{N}^X$ la funzione che associa 1 ad ogni elemento di X avremo che, per ogni $A \in \mathrm{Fin}(X),\ \Sigma(A,1) = \sharp A$.

Se A, B sono sottoinsiemi finiti e disgiunti di X anche $A \cup B$ è un sottoinsieme finito di X, e per ogni $f \in V^X,\ \Sigma(A \cup B, f) = \Sigma(A,f) + \Sigma(A,f)$ come si verifica facilmente per induzione su $\sharp B$. Ma questa osservazione può essere generalizzata come segue

Definizione 2. *Una* partizione *di un insieme X è una famiglia*

$$\mathcal{B} \subseteq \mathcal{P}(X) \text{ tale che } \forall A \neq B \in \mathcal{B},\ A \cap B = \emptyset \text{ e } \bigcup_{A \in \mathcal{B}} A = X$$

Se ogni $A \in \mathcal{B}$ è finito e $f \in V^X$ possiamo definire una funzione $\mathcal{B} \longrightarrow V$ mandando A in $f_A = \Sigma(A, f) = \sum_{a \in A} f(a)$, e quindi, per ogni sottoinsieme finito $\mathcal{C} \subseteq \mathcal{B}$, abbiamo un significato per

$$\sum_{A \in \mathcal{C}} f_A$$

Il caso più importante è quando X stesso è un insieme finito, nel qual caso ogni sua partizione $\mathcal{B}$ è finita, in quanto sottoinsieme di $\mathcal{P}(X)$ e ogni $A \in \mathcal{B}$ è finito in quanto sottoinsieme di X.

Teorema 2. *Se X è un insieme finito, $\mathcal{B}$ è una sua partizione e $f \in V^X$ allora*

$$\sum_{a \in X} f(a) = \sum_{A \in \mathcal{B}} f_A = \sum_{A \in \mathcal{B}} (\sum_{a \in A} f(a))$$

Dimostrazione. Per induzione su $n = \sharp X$. Il caso $n = 0$, cioè $X = \emptyset$ è remarcabilmente sottile e verrà esaminato in dettaglio; i possibili sottoinsiemi di $\mathcal{P}(\emptyset) = \{\emptyset\}$ sono $\mathcal{B} = \emptyset$ e $\mathcal{C} = \{\emptyset\}$. La cretinata logica (implicazione con ipotesi falsa) consente di appurare che entrambe sono partizioni di $\emptyset$ e quindi vanno controllate.

In entrambi i casi avremo che $\sum_{a \in \emptyset} f(a) = 0$; inoltre $\sum_{A \in \mathcal{B}} f_A = 0$ perché si tratta di una somma vuota mentre $\sum_{A \in \mathcal{C}} f_A = 0$ perché è la somma di un solo elemento, e questo è 0 essendo una somma vuota.

Supponiamo ora che il teorema sia vero per tutti gli insiemi con n elementi, che $\sharp X = n + 1$, $f \in V^X$ e $\mathcal{B}$ sia una partizione di X; prendiamo $x \in X$ e sia A l'unico elemento di $\mathcal{B}$ tale che $x \in A$. $\mathcal{C} = \mathcal{B} - \{A\} \cup \{A - \{x\}\}$ è una partizione di $X - \{x\}$, e quindi, per ipotesi induttiva

$$\sum_{a \in X - \{x\}} f(a) = \sum_{B \in \mathcal{C}} f_B = \sum_{B \in \mathcal{B} - \{A\}} f_B + f_{A - \{x\}}$$

da cui segue che

$$\sum_{a \in X} f(a) = \sum_{a \in X - \{x\}} f(a) + f(x) = \sum_{B \in \mathcal{C}} f_B + f(x) =$$

$$(\sum_{B\in\mathcal{B}-\{A\}} f_B + f_{A-\{x\}}) + f(x) = \sum_{B\in\mathcal{B}-\{A\}} f_B + (f_{A-\{x\}} + f(x)) =$$

$$\sum_{B\in\mathcal{B}-\{A\}} f_B + f_A = \sum_{B\in\mathcal{B}} f_B$$

e la dimostrazione è conclusa. □

Questo teorema legalizza il celebre "scambio di sommatorie"che preoccupa gli studenti scrupolosi. Se $X = A \times B$ è un prodotto cartesiano e $f : A\times B \longrightarrow V$ manda (a, b) in f_{ab} allora sia $\left\{A\times\{b\}\right\}_{b\in B}$ che $\left\{\{a\}\times B\right\}_{a\in A}$ sono partizioni di $A \times B$ e quindi

$$\sum_{a\in A}(\sum_{b\in B} f_{ab}) = \sum_{(a,b)\in A\times B} f_{ab} = \sum_{b\in B}(\sum_{a\in A} f_{ab})$$